代 号 10701 学 号 1101120721
分类号 TN 918.1 密 级 公 开

西安電子科技大學

硕士学位论文

题（中、英文）目 最优代数免疫布尔函数的构造与分析

Construction and Analysis of Boolean Functions with Optimal Algebraic Immunity

作者姓名 张欢 指导教师姓名、职务 张卫国 副教授

学科门类 军事学 学科、专业 密码学

提交论文日期 二〇一四年三月

西安电子科技大学
学位论文独创性（或创新性）声明

秉承学校严谨的学风和优良的科学道德，本人声明所呈交的论文是我个人在导师指导下进行的研究工作及取得的研究成果。尽我所知，除了文中特别加以标注和致谢中所罗列的内容以外，论文中不包含其他人已经发表或撰写过的研究成果；也不包含为获得西安电子科技大学或其它教育机构的学位或证书而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中做了明确的说明并表示了谢意。

申请学位论文与资料若有不实之处，本人承担一切相关责任。

本人签名：张欢　　日期 2014.3.14

西安电子科技大学
关于论文使用授权的说明

本人完全了解西安电子科技大学有关保留和使用学位论文的规定，即：研究生在校攻读学位期间论文工作的知识产权单位属西安电子科技大学。本人保证毕业离校后，发表论文或使用论文工作成果时署名单位仍然为西安电子科技大学。学校有权保留送交论文的复印件，允许查阅和借阅论文；学校可以公布论文的全部或部分内容，可以允许采用影印、缩印或其它复制手段保存论文。（保密的论文在解密后遵守此规定）

本学位论文属于保密在___年解密后适用本授权书。

本人签名：张欢　　日期 2014.3.14

导师签名：　　日期 2014.3.14

摘 要

自 2003 年 Courtios 和 Meier 提出了代数攻击以来，在序列密码中，构造布尔函数的指标之一是代数免疫度。于是，构造出代数免疫最优布尔函数受到国内外密码学者的广泛关注。本文主要给出了一种构造代数免疫最优布尔函数的方法，并且给出了两类函数的性能分析，取得了以下主要结果：

(1) 根据 Sihong Su 和 Xiaohu Tang（Designs Codes Cryptography. Published online:01 February 2013）提出的 Reed Muller 码生成矩阵的相关结论，给出了一类基于 Reed Muller 码生成矩阵构造代数免疫最优布尔函数的新方法。证明了代数免疫最优。在此基础上，用 LT 法将函数转化成一阶弹性的。

(2) 介绍了 M-M 和 PS 函数的定义。通过分析得到了以下结论：只有在限制一些条件的情况下，才能构造出高非线性度、代数免疫最优的 M-M 函数。而现在已知的 M-M 函数不是代数免疫最优的。PS_{ap} 函数因为有好的代数结构，都可以修改成高非线性度，代数免疫最优的布尔函数。

关键字：布尔函数 代数免疫 Reed Muller 码 非线性度

Abstract

Because algebraic attack is proposed by Courtios and Meier, in stream ciphers, algebraic immunity is now an important property for Boolean functions. As a result, constructing Boolean functions with optimal algebraic immunity got extensive attention by Scholars at home and abroad .In this paper, we study the method of constructing Boolean functions with optimal algebraic immunity, analyze properties of tow class of functions and obtain the following main results:

(1) Firstly, according to Sihong Su and Xiaohu Tang's paper, which determine the concrete coefficients in the linear expression of the column vectors with respect to a given basis of the generator matrix of Reed Muller code (Designs Codes Cryptography Published online: 01 February 2013), a new method of constructing Boolean functions with optimal algebraic immunity based on the generator matrix of Reed Muller code is given. Secondly, we provide a simper and direct proof for this construction. Last, Boolean functions are changed into 1- resilient functions by LT method.

(2) The constructions of M-M and PS Bent functions are introduced in the text. By analyzing, we get some result. M-M functions with optimal algebraic immunity and high nonlinearity only by a modification under limit of some conditions, but unknown M-M Boolean functions are not optimal. As PS_{ap} Boolean functions have good algebraic structure, the nonlinearity and algebraic immunity are good by modifications.

Keywords: Boolean function Algebraic immunity Reed Muller code Nonlinearity

目 录

第一章 绪论

在信息时代的今天，信息的安全极大地促进了密码学的发展，密码函数已被广泛应用于通信和密码学，特别是在流密码和分组密码的算法设计与分析中占据非常重要的地位。

1.1 密码函数的研究背景和意义

随着计算机技术和通信技术的发展，互联网已经融入了我们的生活，使人们的信息交流，为发展科技，提供了极大的便利，科技，教育，文化和提高人们的生活质量，也给各方面的信息安全带来了巨大的挑战，如国家，组织和个人。由于互联网的开放性，全球性，共享型和动态性，所以任何人都可以轻松地访问，不可避免地会有一些恶意的用户。因此，信息的安全保密成为当前网络发展与应用中亟需解决的问题之一。而密码学是信息安全技术的核心。

密码技术在军事通信的使用和研究已经有几千年了，直到 Shannon1949 年出版的《保密系统的通信理论》[1]，才使得密码系统有了坚实的理论与研究基础，进而使密码学真正成为了一门科学。

密码学主要有两个分支组成，一个是密码编码学，另一个是密码分析学，密码编码学的作用是探索生成高强度的密码算法，实现加密和认证消息。密码分析学的作用是对消息进行破译和伪造，完成窃取机密消息或者对用户进行欺骗破坏活动。这两个分支是相互独立的，但又是相互依存的，就是因为这种关系使得密码学有了的飞速发展。当前，序列密码，分组密码的设计与分析是信息安全领域的热门话题。当前密码体制的研究主要是沿着对称密码体制和公钥密码体制这两个方向发展。公钥密码体制对于通信环境的安全性要求相对比较低，因此它的应用领域越来越广泛。但是它最大的缺点是速度比较慢，而且算法结构比较复杂。对称密码体制是完全相反的，其结构相对简单，且速度快，但它必须双方商量密钥，这就需要解决密钥交换的问题。在现实中，一般同时使用这两种加密密码方案。使用公钥密码体制来生成和交换密钥，使用对称密码体制来处理大部分数据。我们根据加密形式的不同，把对称密码一般可以分为序列密码和分组密码。分组密码的安全性主要取决于 S 盒的盒，可以使用一个多输出布尔函数，所以分组密码的安全问题主要取决于布尔函数的安全。而在考察序列密码时，把它主要分为两部分——一个是驱动部分，另一个是非线性组合部分，驱动部分掌管寄存器的状态转移，技术已经比较完整，因此设计时比较容易，非线性组合的

部分是由一个布尔函数来实现的，于是流密码的安全性的好坏主要是由布尔函数安全性的好坏来决定。所以，布尔函数安不安全直接关系到密码算法本身的安全。

为了密码函数设计的安全性，两个基本原则—混淆和扩散被 Shannon[1]引入了序列密码和分组密码中。主要的目标是抵抗对手对密码系统的系统分析。扩散的作用是尽量把使明文和密文之间的统计相关性变得复杂，使对手没有办法从明文中获得有关密钥的任何信息。混淆的目标是尽量把密文和密钥之间的统计相关性变得复杂，使对手没有办法从明文中获得密钥的任何信息。扩散和混乱，较好地反映了分组密码的基本属性，并成为分组密码的设计理论依据。依据这两条标准，得出了密码算法使用布尔函数的一个基本要求，即：布尔函数必须符合各种密码学指标[2][3][4][5]。当前布尔函数的指标主要包括：平衡性，非线性度，弹性，代数次数，代数免疫等。密码算法对已知的攻击的抵抗性能力我们可以用布尔函数的密码学指标来对其进行测量。所以考虑密码布尔函数的实用功能的指标是对密码算法的安全性非常重要的。

1.2 最优代数免疫布尔函数的发展历史与研究现状

在许多对称密码系统中，布尔函数起着重要的作用。为了抵抗已知的各种攻击，人们提出了许多布尔函数的设计标准。所以布尔函数应该是平衡的，高代数免疫度，高非线性度，高弹性的。代数攻击的提出和发展是近几年在密码分析技术的重要突破，如何抵抗代数攻击已成为学者们关注的焦点。代数攻击一个很好的实例就是对 Toyocrypt 和 LILI-128 等流密码算法的成功攻击[6]。虽然部分密码学者声称代数攻击方法对分组密码也很有效，但目前还没有对分组密码成功攻击的实例。主要原因是分组密码具有迭代结构，多次迭代后的密码算法的代数结构十分复杂，尽管如此，部分学者仍认为代数攻击是对 AES 算法最具有潜在威胁的一种分析方法。2004 年为了衡量密码函数抵抗代数攻击的能力，Courtios 和 Meier 引入了代数免疫度[7]的概念。并且证明 n 元布尔函数的最优代数免疫[8]是 $\left\lceil \frac{n}{2} \right\rceil$。从那以后,最优代数免疫度便成为布尔函数的密码标准之一。最优代数免疫布尔函数的性质和设计方法也随之成为国内外密码学者的普遍关注[9][10][11][12][13]的问题。随后，Courios 提出了快速代数攻击：如果存在低次数的布尔函数 g，使得 fg 的代数次数也比较低，则对于布尔函数 f 快速代数攻

击是容易的。设计布尔函数另一个重要的指标就是有一个比较好的非线性度，它是用来测量函数抵抗快速相关攻击能力的[14]。

在已知具有最优代数免疫的布尔函数中，最简单的函数是由 Ding 首次提出的被称为 MAI 函数[15]：若$wt(x)\geq\left\lceil\frac{n}{2}\right\rceil$，则$F(x)=1$；其它为 0。

2005 年，印度学者 Dalai 等人的 MAI 函数，是用迭代的方法构造的，并首次提出了 MAI 函数一般性构造思路，然后对函数的代数次数，非线性度等密码学性质进行了考察。证明了 MAI 函数 $F(x)$ 是最优代数免疫的。但是根据 Lobanov's 界[16]其非线性度是最坏可能的值。

2005年，Carlet等给出了最优代数免疫布尔函数和 Reed Muller 码的重要关系[17]。他们给出了基于Reed Muller码的生成矩阵构造最优代数免疫布尔函数的充分必要条件。在2007年，通过对MAI函数进行修改，Carlet得到了具备最优代数免疫度的奇变元均衡布尔函数的一般构造方法。

由于不满足其他的密码学性质，几乎所有已知的具有最优代数免疫的布尔函数不能用于密码应用。2008年，Carlet和冯克勤[18]在这方面已经取得了比较大的突破，他们设计了一类代数免疫最优、代数次数最优、高非线性度的n元布尔函数，并且证明至少对于小变元它们能够很好地抵抗快速代数攻击，其非线性度远高于已知MAI函数的非线性度。2009年，涂自然和邓映蒲[19]使用有两个元素的有限域上的二元多项式，而且在Carlet-Feng函数上构造了一类偶变元Bent函数，同时给出了一个尚未证明的猜测，在该猜测成立的基础上，他们设计Bent函数的代数免疫最优。这类函数最大的优点是其非线性度比已知最优代数免疫布尔函数的非线性度都要高随后把其修改成一阶弹性且代数免疫最差为次最优的函数。遗憾的是这种构造不能扩展到奇变元布尔函数。

印度学者Dalai等人给出了代数免疫与汉明重量满足下面的一个关系[9]：设 $f\in B_n$ 且 $AI(f)\geq d$，则 $\sum_{i=0}^{\frac{n}{2}-1}\binom{n}{i}\leq wt(f)\leq\sum_{i=0}^{\frac{n}{2}}\binom{n}{i}$。特别地，当 $AI(f)=\left\lceil\frac{n}{2}\right\rceil$ 时，有：

(1) 当 n 为奇数时，f 必为平衡函数。

(2) 当 n 为偶数时，$\sum_{i=0}^{\frac{n}{2}-1}\binom{n}{i}\leq wt(f)\leq\sum_{i=0}^{\frac{n}{2}}\binom{n}{i}$。

2013年，唐小虎等对Reed Muller码生成矩阵列向量的线性关系给出了完整的证明，并在此基础上给出了基于Reed Muller码生成矩阵构造最优代数免疫布尔函数的一个一般的方法。

目前，构造一类最优代数免疫，高非线性度的布尔函数仍然很困难。需要进一步的分析和研究。

1.3 内容安排及主要结果

论文共分为五章。

第一章 绪论

介绍了密码函数的研究背景、发展历史以及研究现状；介绍了论文的内容安排和作者取得的主要成果。

第二章 基础知识

介绍有限域的定义、布尔函数及其密码学指标。

第三章 代数免疫布尔函数的构造。

给出了代数免疫最优布尔函数的定义和性质，已有的几种构造代数免疫最优函数的方法；提出了一种新的基于 Reed Muller 码的生成矩阵与布尔函数的关系构造代数免疫最优函数的方法，并将其转化为一阶弹性的。

第四章 M-M 类和 PS 类函数的性能分析。

首先介绍了 M-M 函数和 PS 函数的定义和构造方法。接下来对两类函数的密码学指标进行了分析，并且得出了一些相关的结论。

第五章 总结与展望

对构造具备最优代数免疫布尔函数做了归纳，并对以后的研究工作进行了展望和描述。主要研究结果：

(1) 根据 Sihong Su 和 Xiaohu Tang（Designs Codes Cryptography. Published online:01 February 2013）提出的 Reed Muller 码生成矩阵的相关结论，给出了一类基于 Reed Muller 码生成矩阵构造代数免疫最优布尔函数的新方法。并且证明了其代数免疫达到最优。证明了其代数免疫是最优的。在此基础上，用 LT 法转化为一阶弹性的。

(2) 介绍了 M-M 函数和 PS 函数的定义。通过分析得到以下结论：M-M 类函数只有在限制一些条件的情况下，才能构造出高非线性度、代数免疫最优的布尔函数。现在已知的 M-M 函数中大多数不是代数免疫最优的。PS_{ap} 函数因为有好的代数结构，都可以修改成高非线性度，代数免疫最优的布尔函数。

第二章 基础知识

在本文中，许多研究结果是在数学理论的基础上，本章的第一部分介绍了基本的代数知识和有限域等数学知识，第二章介绍了布尔函数的基本概念，基本理论和各种密码学指标。

2.1 有限域

为了引入有限域的定义，我们先介绍群，环，域等基本概念。

定义 2.1 设G是一个非空集合，并在G上定义一个代数运算“$\cdot$”若满足以下条件：

(1) 封闭性：对于任意$a,b\in G$，恒有$a\cdot b\in G$。

(2) 结合律：对于任意元素$a,b,c\in G$有

$$a\cdot(b\cdot c)=(a\cdot b)\cdot c$$

(3) G中有一个元素e，它对于G中任意一个元素a有

$$e\cdot a=a\ （e\text{为左单位元}）$$

(4) G中任意一个元素a都存在G中一个元素b使

$$b\cdot a=e\ （b\text{为左逆元}）$$

则G构成一个群。

群G中所含元素的个数成为群G的阶，记作$|G|$。若群中元素个数有限则称为有限群；否则，称为无限群。若集合只满足(1)和(2)称其为半群。如果群G的运算满足交换律，则称它为交换群或*Abel*群。如果一个群中所有元素都可以由其中一个元素生成，则群称为循环群。循环群必然为*Abel*群。

定义 2.2 交换环是一个具有两中运算“$\cdot$”和“$+$”的代数系统 ，满足以下属性：

(1) $(R,+,\cdot)$关于加法是一个*Abel*群。

(2) $(R,+,\cdot)$的全体非零元素关于其乘法构成一个可交换的半群。

(3) $(R,+,\cdot)$的乘法对加法满足分配律，即对任意三个元素$a,b,c\in R$，有以下式子成立：

$$(b+c)\cdot a=b\cdot a+c\cdot a;\ \ (b+c)\cdot a=b\cdot a+c\cdot a$$

定义 2.3 F是一个非空集合，如果在F上定义了加法“+”和乘法“$\cdot$”两种操作，并满足下列性质：

(1) F在加法运算下式 Abel 群，其单位元简单记为 0；

(2) F中全体非零元素在于乘法运算下是 Abel 群，乘法单位元简单记为 1；

(3) 对于任意 $a,b,c\in \mathrm{F}$，加法和乘法间存在如下分配律：

$$(b+c)\cdot a=b\cdot a+c\cdot a;\quad (b+c)\cdot a=b\cdot a+c\cdot a$$

则称F是一个域。

可以看出域是环的特例。

由有限多个元素组成的集合叫做域，称为有限域，或者称为伽罗瓦（Galois）域。域中所有元素的数目称为这个有限域的阶，用符号 F_q 或者 $GF(q)$ 表示 q 阶有限域。

例如，由1，0两个元素所组成的域称为二元有限域，记为 F_2。

2.2 布尔函数及其密码学指标

本节将给出布尔函数的一些基础知识，主要包括布尔函数的表示方法和密码学性质。关于这方面更详细的论述，可以参考文献[20]。

定义 2.4 设 F_2 是二元有限域，n 为正整数，F_2^n 是 F_2 上的 n 维向量空间，从 F_2^n 到 F_2 的映射 f：$\mathrm{F}_2^n\to\mathrm{F}_2$ 称为 n 元布尔函数。

令 B_n 是所有 n 元布尔函数的集合。易知 B_n 中的元素个数为 2^{2^n}，也就是说，一共有 2^{2^n} 个不同的 n 元布尔函数。

2.2.1 布尔函数的表示方法

从书中可以知道，现在布尔函数的表示方法有很多种，不同的表示在不同的研究背景下都有各自不同的优势，下面我们主要介绍一下四中表示方法：真值表，多项式，小项，以及在有限域上的表示[21]。

I 真值表表示

对于 n 元布尔函数 $f(x):\mathrm{F}_2^n\to\mathrm{F}_2$，$x=(x_1,x_2,\cdots,x_n)$，若是把每一组自变量 $(x_1,x_2,\cdots,x_n)$ 与其相应值列成一个表，则可以获得 F_2 上一个长为 2^n 的向量，该向量就可以称为布尔函数 f 的真值表。习惯上是根据二进制表示 $x_1,x_2,\cdots,x_n$ 值增加从顶部为底的安排真值表。x_n 为最低，x_1 为最高。此时布尔函数 f 的真值表形如：

$$(f(0,\cdots,0,0),f(0,\cdots,0,1),f(0,\cdots,1,0),\cdots f(1,\cdots,1,1))$$

我们可以真值表唯一地表示每一个布尔函数。该向量中全体1的数目称为 $f(x)$ 的汉明(Hamming)重量，记为 $wt(f)$。若 n 元布尔函数满足 $wt(f)=2^{n-1}$，则称 $f(x)$ 是平衡函数。同时称支撑集 $Supp(f)$ 为使得 $f(x)=1$ 的 x 取值的集合，即

$$Supp=\left\{x\in\mathrm{F}_2^n\mid f(x)=1\right\}$$

可知，$wt(f)=|Supp(f)|$。

II 小项表示

对于 $x_i,c_i\in \mathrm{F}_2$，约定 $x_i^1=x_i,x_i^0=\overline{x_i}=1+x_i$，于是

$$x_i^{c_i}=\begin{cases}1, & x_i=c_i\\ 0, & x_i\neq c_i\end{cases}$$

设整数 $c\ (0\le c\le 2^n-1)$ 的二进制表示是 $c_1,c_2,\cdots,c_n$，约定 $x^c=x_1^{c_1}x_2^{c_2}\cdots x_n^{c_n}$，它具有下述的“正交性”

$$x_1^{c_1}x_2^{c_2}\cdots x_n^{c_n}=\begin{cases}1, & (x_1,x_2,\cdots,x_n)=(c_1,c_2,\cdots,c_n)\\ 0, & (x_1,x_2,\cdots,x_n)\neq(c_1,c_2,\cdots,c_n)\end{cases}\tag{2-1}$$

由此可得到

$$f(x)=\sum_{c=0}^{2^n-1}f(c_1,c_2,\cdots,c_n)x_1^{c_1}x_2^{c_2}\cdots x_n^{c_n}\tag{2-2}$$

式（2-2）就是函数 f 的小项表示，每一个被加项 $f(c_1,c_2,\cdots,c_n)x_1^{c_1}x_2^{c_2}\cdots x_n^{c_n}$ 称为一个小项。其中求和符号是指模 2 加。

III 代数正规型(ANF)表示

每一个 n 元布尔函数 $f\in B_n$ 都可以唯一地表示为：

$$\begin{aligned}f(x_1,x_2,\cdots,x_n)&=a_0+\sum_{i=1}^{n}a_ix_i+\sum_{1\le i<j\le n}a_{i,j}x_ix_j+\cdots\\&+\sum_{1\le i_1<\cdots<i_d\le n}a_{i_1,\cdots,i_d}x_{i_1}\cdots x_{i_d}+\cdots+a_{1,\cdots,n}x_1\cdots x_n\end{aligned}\tag{2-3}$$

其中，$a_0,a_i,a_{i,j},\cdots,a_{1,\cdots,n}\in \mathrm{F}_2$。

式（2-3）表示的形式为 f 的代数正规型（Algebraic Normal Form, ANF）。记集合 $N=\{1,2,\cdots,n\}$，用 $P(N)$ 表示 N 的幂集，即 N 的所有幂集构成的集合，则 f 的代数正规型可表示为：

$$f(x_1,x_2,\cdots,x_n)=\sum_{I\in P(N)}a_I\Big(\prod_{i\in I}x_i\Big)=\sum_{I\in P(N)}a_Ix^I\tag{2-4}$$

其中，$x^I=\prod_{i\in I}x_i$。

非零布尔函数 f 的代数正规型中所有不是0的系数所含变元个数最多的数目就是它的代数次数，记为 $\deg f$，即

$$\deg f=\max\left\{|I||a_I\neq 0,I\in P(N)\right\} \tag{2-5}$$

规定零函数的代数次数为0，如果 $\deg f\leq 1$，则 f 称为仿射函数。

全体 n 元仿射函数的集合记为 A_n，即

$$A_n=\left\{f(x_1,x_2,\cdots,x_n)=\sum_{i=1}^{n}a_ix_i+a_0\middle|a_0,a_1,a_2,\cdots,a_n\in \mathrm{F}_2\right\} \tag{2-6}$$

其中，没有常数项的仿射函数称为线性函数， n 元线性函数的全体集合记为 L_n，即

$$L_n=\left\{f(x_1,x_2,\cdots,x_n)=\sum_{i=1}^{n}a_ix_i\middle|a_1,a_2,\cdots,a_n\in \mathrm{F}_2\right\} \tag{2-7}$$

IV 有限域 F_{2^n} 上布尔函数的表示

令 α 是 F_{2^n} 上的本原元， n 元布尔函数 $f(x)$ 定义为从 F_{2^n} 到 F_2 的映射，即其真值表可以表示为 $f(0),f(1),f(\alpha),\cdots,f\left(\alpha^{2^n-2}\right)$，与代数正规型形式相同的 n 元布尔函数 $f(x)$ 也可以惟一的表示成有限域 F_{2^n} 上的一元多项式，即 $f(x)=\sum_{i=0}^{2^n-1}a_ix^i$。

2.2.2 布尔函数的密码学指标

Walsh 变换也称为 Walsh 谱，是考察布尔函数密码学指标重要的数学用具之一。

定义 2.5 设 n 维布尔函数 $f(x)$，定义

$$W_f(\omega)=\sum_{x\in \mathrm{F}_2^n}(-1)^{f(x)+x\cdot\omega},\omega\in \mathrm{F}_2^n \tag{2-8}$$

则称 $W_f(w)$ 是 $f(x)$ 的 *wash* 变换。其中“·”表示两个 n 维向量的点积，即 $x\cdot\omega=\sum_{1\leq i\leq n}x_i\omega_i$

其中， $x=(x_1,x_2,\cdots,x_n)\in \mathrm{F}_2^n$， $\omega=(\omega_1,\omega_2,\cdots,\omega_n)\in \mathrm{F}_2^n$。

I 非线性度

为了抵抗线性密码攻击，密码体制中所使用的布尔函数应该离所有仿射函数的距离尽可能大。

定义 2.6 布尔函数 f 的非线性度 N_f 的定义是布尔函数 f 与所有仿射函数的最小 Hamming 距离，即

$$N_f = \min_{g \in A_n} d(f,g)$$

从密码学角度来看，非线性度越高的布尔函数抵抗线性攻击的能力就越强，由（2-6）式可知 $\max_{w \in F_2^n} |W_f(w)|$ 要尽可能的小。

定理 2.1 （Parseval 恒等式） 设任意 n 元布尔函数 $f(x)$，则下式成立：

$$\sum_{\omega \in F_2^n} W_f^2(\omega) = 2^{2n} \tag{2-9}$$

由 Parseval 恒等式可知知道，对于任意 n 元布尔函数 f，有下式成立：

$$\max_{\omega \in F_2^n} |W_f(\omega)| \geq 2^{n/2},$$

即

$$N_f \leq 2^{n-1} - 2^{\frac{n}{2}-1}.$$

当 $N_f = 2^{n-1} - 2^{\frac{n}{2}-1}$ 时，有 $W_f(\omega) = \pm 2^{\frac{n}{2}}$，此时布尔函数 f 称为 Bent 函数。注意到布尔函数的非线性度是一个整数，故只有当 n 时偶数时，Bent 函数才可能存在。

II 相关免疫和弹性[23]

相关免疫的概念是由 Siegenthaler[5]提出的，其主要是用来防止密码分析者或攻击者对流密码中的各种算法进行相关攻击。

定义 2.7 设 n 元布尔函数 $f(x_1, x_2, \cdots, x_n)$，其中 $x_1, x_2, \cdots, x_n$ 是 F_2 上均匀分布的随机变量，如果 f 与 $x_1, x_2, \cdots, x_n$ 中任意 m 个变元 $x_{i_1}, x_{i_2}, \cdots, x_{i_m}$ 是统计独立的，则对任意变量 $(a_1, a_2, \cdots, a_m) \in F_2^m (m \leq n)$ 和 $a \in F_2$，有下式成立：

$$P\left(f = a \mid x_{i_1} = a_1, x_{i_2} = a_2, \cdots, x_{i_m} = a_m\right) = P(f = a) \tag{2-10}$$

则称 f 是 m 阶相关免疫函数（Correlation Immune）。

m阶弹性函数是指布尔函数是平衡的m阶相关免疫函数，但如果函数是平衡的但没有相关免疫阶，则可以看成是0阶弹性函数。

定理 2.2[22]（Xiao-Massey 定理）设$f(x)=f(x_1,x_2,\cdots,x_n)$是一个$n$元布尔函数，其中$x_1,x_2,\cdots,x_n$是$F_2$上均匀分布的独立随机变量，则$f(x)$是$t$阶相关免疫函数当且仅当对任意$a\in F_2^n$，$1\le wt(\alpha)\le t$的$\alpha$，均有：

$$W_f(\alpha)=0 \tag{2-11}$$

定理 2.3 给定一个n元布尔函数$f(x)=f(x_1,x_2,\cdots,x_n)$，若$f(x)$既$m\ (1\le m\le n-1)$阶弹性函数，则$\deg f\le n-m-1$；若$f(x)$是$m$阶相关免疫函数，则$\deg f\le n-m$。

III 雪崩效应与扩散准则

在研究S盒时，Webster[24]将“完全性”和“雪崩效应”两个概念组合成了一个新的概念称为严格雪崩准则，简记为SAC。

设任意n元布尔函数$f(x)$，$\alpha\in F_2^n$，用$D_f(\alpha)=f(x)+f(x+\alpha)$表示$f(x)$在$\alpha$的差分：

(1) 使$D_f(\alpha)$为常数的α，则称为$f(x)$的线性结构。

(2) 如果满足$wt(\alpha)=1$的α，都使得$D_f(\alpha)$为平衡函数，则称$f(x)$满足严格雪崩，记为SAC。

(3) 如果满足$1\le wt(\alpha)\le k$的α，都使得$D_f(\alpha)$为平衡函数，则称$f(x)$满足k次扩散准则，记为$PC(k)$。

IV 代数免疫度

2003年Courtios和Meier在文献[25]中提出了两种新的攻击思想，指出如果滤波函数f具有如下两个缺陷，一个是存在布尔函数g，使得布尔函数fg代数次数比较低；另一个是存在布尔函数g，使得fg以很大的概率接近于一个低次数的布尔函数h。那么同样可以对滤波序列实施代数攻击。

文献[25]中主要讨论了基于上述第一个缺陷的代数攻击，并给出了攻击中可以利用的三种情形：

情况A 存在较低次布尔函数g_1，使得$h_1=fg_1$的代数次数也比较低；

情况B 存在低次布尔函数g_2，使得布尔函数$fg_2=0$；

情况C 存在较高次数的布尔函数g_3，使得布尔函数$h_2=fg_3$的代数次数也比较低。

这三种情形实际可以归结为一种情形，即代数攻击能否有效实施的关键是情形 B 中低次布尔函数是否存在。

2004 年 *Meier* 等人将代数攻击归纳为找布尔函数的非零零化子。也就是说，标准代数攻击主要是找到布尔函数 f 和 $f+1$ 的不是 0 的零化子中代数次数最低的那个次数。此最低数目就是 f 的代数免疫度(Algebraic Immunity)。从某种程度而言，我们可以用代数免疫度来测量布尔数抵抗代数攻击的本领。从此代数免疫得到的密码学界的广泛关注，高代数免疫成为布尔函数的密码学指标之一[26]。

定义 2.8 设 $f,g\in B_n$，如果 $fg=0$，就称 g 是 f 的零化子。对于任意的函数 $f\in B_n$，记 $Ann(f)$ 是其零化子的集合，即

$$Ann(f)=\{g\in B_n \mid fg=0\} \tag{2-12}$$

定义 2.9 设 $f\in B_n$，$AI(f)$ (Algebraic Immunity, AI)表示 f 或者 $f+1$ 非零零化子 g 的最小代数的次数，即

$$AI(f)=\min\left\{\deg g \middle| 0\neq g\in Ann(f)\cup Ann(1+f)\right\} \tag{2-13}$$

定理 2.4 设 f 是一个 n 元布尔函数，则 f 的代数免疫度满足：

$$AI(f)\leq \min\left\{\left\lceil\frac{n}{2}\right\rceil,\deg f\right\} \tag{2-14}$$

其中，$\lceil x\rceil$ 表示对实数 x 取上整，即不小于 x 的最小整数。

定义 2.10 一个 n 元布尔函数的代数免疫度是 $\left\lceil\frac{n}{2}\right\rceil$，称该布尔函数拥有最优代数免疫度或最大代数免疫度(Maximum Algebraic Immunity)，简称 MAI 函数。

定理 2.5 设 $f\in B_n$，$AI(f)=d$，则

$$N_f(f)\geq 2^{n-1}-\sum_{i=d-1}^{n-d}\binom{n-1}{i}=2\sum_{i=0}^{d-2}\binom{n-1}{i} \tag{2-15}$$

代数免疫度高是抵抗代数攻击的必要条件但不是充分条件，假如存在两个代数次

数比较低的布尔函数 $g, h \neq 0$，满足 $fg = h$，则快速代数攻击是比较简单的。一个 n 元布尔函数 f 能够抵挡快速代数攻击，假设没有非零布尔函数 g 和 h 满足 $fg = h$ 和 $\deg(g)+\deg(h)<n, \deg(g)<\frac{n}{2}$。

V Reed Muller 码和最优代数免疫布尔函数的联系

在研究密码函数的性质，构造与应用时，需要用到一些纠错码的知识，特别是与布尔函数密切相关的线性码—Reed Muller 码[27][28]。

假设 $\alpha_1, \alpha_2, \cdots, \alpha_{2^n}$ 是 F_2 上的所有 n 维向量，它们是按照汉明重量和字典顺序排列

即，$\alpha_1=(0,0,0,0,\cdots,0), \alpha_2=(1,0,0,0,\cdots,0), \alpha_3=(0,1,0,0,\cdots,0), \cdots, \alpha_{n+1}=(0,0,0,0,\cdots,1)$

$\alpha_{n+2}=(1,1,0,0,\cdots,0), \alpha_{n+3}=(1,0,1,0,\cdots,0), \alpha_{n+4}=(1,0,0,1,\cdots,0), \cdots, \alpha_{\binom{n}{2}+n+1}=(1,0,0,0,\cdots,1)$

$, \cdots, \alpha_{2^n}=(1,1,1,\cdots,1)$.很容易证明 $wt(\alpha_i) \leq k$，当且仅当 $1 \leq i \leq \sum_{j=0}^{k}\binom{n}{j}$。因此，代数次数小于等于 k 的布尔函数 f 的代数正规型也可以表示成

$$f(x)=\bigoplus_{i=1}^{s} c(\alpha_i)x^{\alpha_i} \tag{2-16}$$

其中，$s=\sum_{i=0}^{k}\binom{n}{i}, c(\alpha_i) \in F_2$，因此，$\deg\left(x^{\alpha_i}\right) \leq k$，当且仅当 $wt(\alpha_i) \leq k$。

定义 2.11 代数次数小于等于 k 的 n 元布尔函数的全体集合成为 $k\ (1 \leq k \leq n)$ 阶 Reed Muller 码，记作 $RM(k,n)$。

显然，Reed Muller 码是 F_2 上的 $\sum_{i=0}^{k}\binom{n}{i}$ 维向量空间，单项式的次数至多是 k，即

记 $\Gamma_k=\left\{x^{\alpha_i} \mid 1 \leq i \leq \sum_{j=0}^{k}\binom{n}{j}\right\}$ 是 Reed Muller 码的基。

定义一个映射 ψ：$\Gamma_k \to F_2^{2^n}$

$$\psi\left(x^{\alpha_i}\right)=\left[\alpha_1^{\alpha_i},\alpha_2^{\alpha_i},\cdots,\alpha_{2^n}^{\alpha_i}\right]$$

它是 x^{α_i} 的真值表，$1\le i\le\sum_{j=0}^{k}\binom{n}{j}$。考虑下面的 $\sum_{j=0}^{k}\binom{n}{j}\times 2^n$ 矩阵：

$$G(k,n)=\begin{pmatrix}\psi\left(x^{\alpha_1}\right)\\ \psi\left(x^{\alpha_2}\right)\\ \vdots\\ \psi\left(x^{\alpha_s}\right)\end{pmatrix}=\begin{pmatrix}\alpha_1^{\alpha_1} & \alpha_2^{\alpha_1} & \cdots & \alpha_{2^n}^{\alpha_1}\\ \alpha_1^{\alpha_2} & \alpha_2^{\alpha_2} & \cdots & \alpha_{2^n}^{\alpha_2}\\ \vdots & \vdots & \ddots & \vdots\\ \alpha_1^{\alpha_s} & \alpha_2^{\alpha_s} & \cdots & \alpha_{2^n}^{\alpha_s}\end{pmatrix} \tag{2-17}$$

其中 $s=\sum_{i=0}^{k}\binom{n}{i}$。当 n 为奇数时，若 $k=\left\lceil\frac{n}{2}\right\rceil-1$，则 $\sum_{i=0}^{k}\binom{n}{i}=2^{n-1}$；当 n 为偶数时，$\sum_{i=0}^{k}\binom{n}{i}=2^{n-1}-\binom{n-1}{\frac{n}{2}}$。

根据矩阵 $G(k,n)$ 很容易证明任一个布尔函数 $f\in B_n,\deg(f)\le k$，有

$$\left[f(\alpha_1),\cdots,f\left(\alpha_{2^n}\right)\right]=\left[c(\alpha_1),\cdots c\left(\alpha_{2^n}\right)\right]G(k,n) \tag{2-18}$$

即，$G(k,n)$ 是 Reed Muller 码 $RM(k,n)$ 的生成矩。

给定 n 元布尔函数 f 和正整数 $k\le n$，定义 G 为 k 阶 Reed Muller 码 $RM(k,n)$ 的生成矩阵 $G(k,n)$，$R_f^{(1)}(k,n)\left(R_f^{(0)}(k,n)\right)$ 是 G 中包含所有第 $i\ (1\le i\le n)$ 列向量，且满足 $a_i\in\mathrm{supp}(f)\ \left(a_i\in\left(\mathrm{F}_2^n-\mathrm{supp}(f)\right)\right)$ 的子矩阵。显然，矩阵 $R_f^{(1)}(k,n)\left(R_f^{(0)}(k,n)\right)$ 有 $\sum_{i=0}^{k}\binom{n}{i}$ 行 $wt(f)\left(2^n-wt(f)\right)$ 列。

定理 2.6 令 $k=\left\lceil\frac{n}{2}\right\rceil-1$，$n$ 元布尔函数 f 具备代数免疫最优的充要条件是 $\sum_{i=0}^{k}\binom{n}{i}\times\sum_{i=0}^{k}\binom{n}{i}$ 阶矩阵 $R_f^{(1)}(k,n)\left(R_f^{(0)}(k,n)\right)$ 是可逆矩阵。

对于任意两个向量$\alpha=(a_1,a_2,\cdots,a_n),\beta=(b_1,b_2,\cdots,b_n)\in \mathrm{F}_2^n$，称$\beta$覆盖$\alpha$，如果对于所有$1\le i\le n$，都有$a_i\le b_i$，记为$\alpha\preceq\beta$。令$\beta^\alpha=b_1^{a_1}b_2^{a_2}\cdots b_n^{a_n}$且$0^0=1^1=1^0=1$，显然，$\beta^\alpha=1$当且仅当$\alpha\preceq\beta$。

VI Reed Muller码生成矩阵G中列向量的线性表示

首先假设$k=\left\lceil\frac{n}{2}\right\rceil-1,s=\sum_{i=0}^{k}\binom{n}{i}$，根据式（2-17），可以得到Reed Muller码生成矩阵G的第j列向量可以表示成$\left(\alpha_j^{\alpha_1},\alpha_j^{\alpha_2},\cdots,\alpha_j^{\alpha_s}\right)^T$，$1\le j\le 2^n$。

一般，用c_{α_j}表示生成矩阵G的第j列向量，即

$$c_{\alpha_j}=\left(\alpha_j^{\alpha_1},\alpha_j^{\alpha_2},\cdots,\alpha_j^{\alpha_s}\right)^T$$

因此，式（2-17）中的生成矩阵G能被表示成$G=\left(c_{\alpha_1},c_{\alpha_2},\cdots,c_{\alpha_{2^n}}\right)$。

按照定理2.5，构造具备最优代数免疫布尔函数$f\in B_n$且$wt(f)=s$的必要条件是找到矩阵G中秩为s的子矩阵$R_f^{(1)}(k,n)$。矩阵G在基$\left(c_{\alpha_1},c_{\alpha_2},\cdots,c_{\alpha_{2^n}}\right)$下列向量的线性表示

对于检验$R_f^{(1)}(k,n)$的秩是否为s很有用。

定理2.7[27] 对任意向量$u\in \mathrm{F}_2^n$，满足$wt(u)=k+j,1\le j\le n-k$，有

$$c_u=\bigoplus_{i=0}^{k}a_i^{(j)}\left(\bigoplus_{\substack{\alpha\preceq u\\ wt(\alpha)=k-i}}c_\alpha\right) \tag{2-19}$$

其中，$a_i^{(j)}\in \mathrm{F}_2^n,0\le i\le k$，满足

$$a_0^{(j)}=1,\quad a_i^{(j)}=1\oplus\bigoplus_{l=0}^{i-1}a_l^{(j)}\binom{i+j}{i-l},\quad 1\le i\le k \tag{2-20}$$

定理 2.8[27] 令$u \in \mathrm{F}_2^n$且$wt(u)=k+j\ (1 \le j \le n-k)$，在式(2-20)$c_a$的线性表示中，$c_\alpha(\alpha \preceq u, wt(\alpha)=k+j)$的系数$a_i^{(j)}$满足

$$a_i^{(j)} = \binom{i+j-1}{i} (\mathrm{mod}\, 2) \tag{2-21}$$

第三章 代数免疫度最优布尔函数的构造

最优代数免疫布尔函数是能够抵抗代数攻击的密码函数。本章主要给出了一种基于 Reed Muller 码的生成矩阵构造具备最优代数免疫的布尔函数的方法。

3.1 几种常见的代数免疫度最优布尔函数的构造

目前已经有了很多种关于 MAI 函数的构造方法，这些方法按其构造思路的不同可以分为以下几类：基于支撑包含关联的构造方法，基于平面理论的构造方法，基于交换基技术的构造方法，基于有限域表示的构造方法等。

3.1.1 基于支撑集包含关系构造 MAI 函数

Dalai 于 2005 年提出了一种基于支撑包含关系构造 MAI 函数的方法[28]，其主要思想来自于以下引理：

引理 3.1.1[29] 设 $f, f_1, f_2 \in B_n$，满足如下条件：

(1) f_1, f_2 没有代数次数低于 $\left\lceil \frac{n}{2} \right\rceil$ 的非零零化子。

(2) $\mathrm{supp}(f) \supseteq \mathrm{supp}(f_2), \mathrm{supp}(f+1) \subseteq \mathrm{supp}(f_1)$。

则，$AI(f) = \left\lceil \frac{n}{2} \right\rceil$。

引理 3.1.2[29] 设 $f \in B_n$，$AI(f) = \left\lceil \frac{n}{2} \right\rceil$，则存在 $f_1, f_2 \in B_n$ 使得

$$\mathrm{supp}(f) \supseteq \mathrm{supp}(f_2),$$

$$\mathrm{supp}(f+1) \subseteq \mathrm{supp}(f_1),$$

$$wt(f_1) = wt(f_2) = \sum_{i=0}^{\left\lceil \frac{n}{2} \right\rceil - 1} \binom{n}{i},$$

并且 f_1, f_2 都没有代数次数低于 $\left\lceil \frac{n}{2} \right\rceil$ 的不为零的零化子。

引理 3.1.3[29] 设 $f_1, f_2 \in B_n$，$f_1(x)=\begin{cases}1, & wt(x)<\left\lceil\frac{n}{2}\right\rceil\\ 0, & wt(x)\geq\left\lceil\frac{n}{2}\right\rceil\end{cases}$，当 n 为偶数时，令 $f_2(x)=$

$\begin{cases}1, & wt(x)\leq\left\lceil\frac{n}{2}\right\rceil\\ 0, & wt(x)>\left\lceil\frac{n}{2}\right\rceil\end{cases}$，则 f_1, f_2 都没有代数次数低于 $\left\lceil\frac{n}{2}\right\rceil$ 的非零零化子。

构造 1[29] 设 $f \in B_n$，当 n 为奇数时，令

$$f(x)=\begin{cases}1, & wt(x)<\left\lceil\frac{n}{2}\right\rceil\\ 0, & wt(x)\geq\left\lceil\frac{n}{2}\right\rceil\end{cases}, \tag{3-1}$$

当 n 为偶数时，令

$$f(x)=\begin{cases}1, & wt(x)<\left\lceil\frac{n}{2}\right\rceil\\ 0, & wt(x)\geq\left\lceil\frac{n}{2}\right\rceil\\ b\in\{0,1\}, & wt(x)=\left\lceil\frac{n}{2}\right\rceil\end{cases}, \tag{3-2}$$

则两类布尔函数都满足 $AI(f)=\left\lceil\frac{n}{2}\right\rceil$。

3.1.2 基于有限域表示构造 MAI 函数

Carlet 和冯克勤在 2008 年提出了构造 MAI 函数的一种新方法[18]，其构造的主要思路是使用了有限域 F_{2^n} 上的乘法群，称为“基于有限域表示的构造方法”。

定理 3-1[18] 设 $n\geq 2$，是一个正整数，α 是有限域 F_{2^n} 上的生成元，f 是 F_{2^n} 上支撑为 $\{0\}\cup\{\alpha^i, i=0,1,\cdots,2^{n-1}-2\}$ 的布尔函数，则 f 具备最优代数免疫度 $\left\lceil\frac{n}{2}\right\rceil$，且

$$N_f \geq 2^{n-1}+\frac{2^{\frac{n}{2}+1}}{\pi}\ln\left(\frac{\pi}{4\left(2^n-1\right)}\right)-1\approx 2^{n-1}-\frac{2\ln 2}{\pi}n2^{\frac{n}{2}}。$$

受到 Carlet 和冯克勤相关工作的启迪，一类 PS 型 Bent 函数被涂自然和邓映蒲证明。

猜想[19] 设 $k\in\mathbf{Z},k>1$，对任意 $x\in\mathbf{Z}_{2^k-1}$，把 x 展开成 k 位二进制数，用 $wt(x)$ 表示 x 的展开式中 1 的个数，对任意 $t\in\mathbf{Z},0<t<2^k-1$，令

$$S_t=\left\{(a,b)\mid a,b\in\mathbf{Z}_{2^k-1},a+b\equiv t \bmod 2^k-1,wt(a)+wt(b)\leq k-1\right\} \quad (3\text{-}3)$$

则 $|S_t|\leq 2^{k-1}$。

构造 3.1[19] 设 $n=2k,\alpha$ 是 F_{2^k} 的本原元，布尔函数 $g:\mathrm{F}_{2^k}\to\mathrm{F}_2$，取支撑 $\mathrm{supp}(g)=\left\{\alpha^s,\alpha^{s+1},\cdots,\alpha^{s+2^k-1}\right\}$，其中 $0\leq s\leq 2^k-1,f:\mathrm{F}_{2^k}\times\mathrm{F}_{2^k}\to\mathrm{F}_2$，令

$$f(x,y)=\begin{cases}g\left(xy^{-1}\right), & xy\neq 0\\ 0, & \text{否则}\end{cases} \quad (3\text{-}4)$$

在猜想成立的前提下，函数 $f(x,y)$ 为 n 元 Bent 函数，且 $AI(f)=k=\frac{n}{2}$。随后，他们对该构造进行了改进，改进后的函数为平衡函数。

构造 3.2[19]设 $n=2k,\alpha$ 是 F_{2^k} 的本原元，布尔函数 $g:\mathrm{F}_{2^k}\to\mathrm{F}_2$，取支撑 $\mathrm{supp}(g)=\left\{\alpha^s,\alpha^{s+1},\cdots,\alpha^{s+2^k-1}\right\}$，其中 $0\leq s\leq 2^k-1,f:\mathrm{F}_{2^k}\times\mathrm{F}_{2^k}\to\mathrm{F}_2$，令

$$f(x,y)=\begin{cases}g\left(xy^{-1}\right), & xy\neq 0\\ 1, & x=0,y\in\delta\\ 0, & \text{否则}\end{cases} \quad (3\text{-}5)$$

其中，$\delta=\left\{\alpha^i\mid i=2^{k-1}-1,2^{k-1},\cdots,2^k-2\right\}$。则函数 $f(x,y)$ 为平衡函数，代数次数为 $n-1$，非线性度 $N_f\geq 2^{n-1}-2^{\frac{n}{2}-1}-2^{\frac{k}{2}}k\ln 2-1$，且在猜想成立的前提下为 MAI 函数。

3.1.3 基于正整数插值构造 MAI 函数

该构造的主要思想是：将 F_2^n 上的元素与区间 $\left[0,2^n-1\right]$ 上的整数一一对应起来，更

准确的说，是将 $X=(x_1,x_2,\cdots,x_n)\in \mathrm{F}_2^n$ 对应于整数 $\sum_{i=1}^{n}x_i2^{i-1}$。定义 $Y_1,Y_2\in \mathrm{F}_2^n$，$[Y_1,Y_2)=\{Y\in \mathrm{F}_2^n \mid Y_1\le Y<Y_2\}$。记 Y_0 到 Y_k 为 F_2^n 上所有汉明重量不超过 $\lceil n/2\rceil-1$ 的元素按升序排列，从而有 $k=\sum_{i=0}^{\lceil n/2\rceil-1}\binom{n}{i}-1$。

引理 3.1.4 设 n 是偶数，如果 f 是 Hamming 重量等于 $\sum_{i=0}^{\lceil n/2\rceil-1}\binom{n}{i}$ 的 n 元布尔函数，则 $AI(f)=n/2$ 的充要条件是 f 不存在次数小于 $\frac{n}{2}$ 的非零零化子。

引理 3.1.5[30] 考虑一个 d 次单项式函数 $f(x)=x_1^{y_1}x_2^{y_2}\cdots x_n^{y_n}$，令 $Y=(y_1,y_2,\cdots,y_n)$，以下成立，对 $[0,Y)$ 中的任意的变量 X，都有 $f(X)=0$；对 $\left[Y,Y^{'}\right)$ 中的任意 X，都有 $f(X)=1$，其中，$Y^{'}\in \mathrm{F}_2^n$ 是大于 Y 且重量不超过 d 的第一个元素。

构造 4.1[30]

(1) 从 $i=0$ 到 $k-1$，任选元素 $X_i\in[Y_i,Y_{i+1})$；

(2) 若 $i=k$，任意元素 X_i，使得 $\mathrm{supp}(Y_i)\subset \mathrm{supp}(X_i)$；

(3) 布尔函数 $f\in B_n$，使得 $\mathrm{supp}(f)=\bigcup_{i=0}^{k}\{X_i\}$。

则 $AI(f)=\left\lceil\frac{n}{2}\right\rceil$。

构造 4.2[30]（当 n 为偶数时）

(1) 从 $i=0$ 到 $k-1$，任选元素 $X_i\in[Y_i,Y_{i+1})$ 且 $wt(X_i)\le\frac{n}{2}$；

(2) 若 $i=k$，任意元素 X_i，使得 $\mathrm{supp}(Y_i)\subset \mathrm{supp}(X_i)$ 且 $wt(X_i)\le\frac{n}{2}$；

(3) 从 $i=k+1$ 到 $2^{n-1}-1$，任选元素 $X_i\notin\bigcup_{j=0}^{2^{n-1}-1}\{X_j\}$ 且 $wt(X_i)\le\frac{n}{2}$；

(4) 布尔函数 $f \in B_n$，使得 $\mathrm{supp}(f)=\bigcup_{i=0}^{2^{n-1}-1}\{X_i\}$。

则 $AI(f)=\frac{n}{2}$。

3.1.4 基于 Reed Muller 码的生成矩阵构造 MAI 函数

在文献[27]中为了简便起见，定义

$$\begin{cases} W^{\le k}=\{\alpha \in \mathrm{F}_2^n \mid wt(\alpha)\le k\} \\ W^{\ge k}=\{\alpha \in \mathrm{F}_2^n \mid wt(\alpha)\ge k\}, 0\le i\le n \\ W^{=k}=\{\alpha \in \mathrm{F}_2^n \mid wt(\alpha)=k\} \end{cases} \tag{3-6}$$

根据定理 2-5，构造 n 元具备最优代数免疫布尔函数 $f\ (wt(f)=s)$ 等价于找到式（2-17）中生成矩阵 G 的 $s\times s$ 阶非奇异矩阵。例如，$[c_{\alpha_1},c_{\alpha_2},\cdots,c_{\alpha_s}]$ 是一个这样的子矩阵。一般的方法是修改这个矩阵并且得到另一个可逆矩阵。更准确地说，对于一个正整数 $1\le l\le s$，挑选两个向量子集 $U=\{u_1,u_2,\cdots,u_l\}\subseteq W^{\ge k}, T=\{\beta_1,\beta_2,\cdots,\beta_l\}\subseteq W^{\le k}$，令 $W^{\le k}\setminus T=\{\gamma_1,\gamma_2,\cdots,\gamma_{s-l}\}$。

根据基 $\{c_{\beta_1},c_{\beta_2},\cdots,c_{\beta_l},c_{\gamma_1},c_{\gamma_2},\cdots,c_{\gamma_{s-l}}\}$，子矩阵 $[c_{u_1},c_{u_2},\cdots,c_{u_l},c_{\gamma_1},c_{\gamma_2},\cdots,c_{\gamma_{s-l}}]$ 能表示成

$$[c_{u_1},c_{u_2},\cdots,c_{u_l},c_{\gamma_1},c_{\gamma_2},\cdots,c_{\gamma_{s-l}}]=[c_{\beta_1},c_{\beta_2},\cdots,c_{\beta_l},c_{\gamma_1},c_{\gamma_2},\cdots,c_{\gamma_{s-l}}]\begin{pmatrix} B & 0 \\ C & I \end{pmatrix} \tag{3-7}$$

其中，$B=(b_{i,j})$ 是一个 $l\times l$ 阶矩阵，0 是零矩阵，I 是阶为 $s-l$ 的单位矩阵。因此，关键问题是找到两个向量子集 U 和 T 使得 B 是个可逆矩阵。

一般来说，确定矩阵 B 的秩是不容易的，但是如果 B 是一个上三角矩阵或者下三角矩阵，则很容易确定矩阵的秩。所以问题的关键是找到两个向量子集 $U=\{u_1,u_2,\cdots,u_l\}\subseteq W^{\ge k}, T=\{\beta_1,\beta_2,\cdots,\beta_l\}\subseteq W^{\le k}$，满足下面的两个条件 C_1 和 C_2。

C_1：在 c_{u_i} 的线性表示中 c_{β_i} 的系数是 1，其等价于 $b_{i,i}=1$，$1\le i\le l$。

C_2：在c_{u_j}的线性表示中c_{β_j}的系数是0，其等价于$b_{i,j}=0$，$1\le j<i\le l$，$(1\le i<j\le l)$。

构造5[31]令n是奇数，对于任意整数l，$1\le l\le\binom{n}{k}$，两个子集$U=\{u_1,u_2,\cdots,u_l\}\subseteq W^{\ge k}$,$T=\{\beta_1,\beta_2,\cdots,\beta_l\}\subseteq W^{\le k}$

(1) 如果$1\le i\le l$时，$\beta_i\preceq u_i$。

(2) 如果$1\le j<i\le l$时，$\beta_i\not\preceq u_i$，则布尔函数$f\in B_n\left(\mathrm{supp}(f)=\left(W^{\le k}\setminus T\right)\cup U\right)$有最优代数免疫。

在文献中，作者Su sihong，唐小虎等也给出了基于Reed Muller码的生成矩阵构造最优代数免疫度布尔函数的方法。

*Dalai*等在2005年第一次提出了一种递归构造法[9]，其是从二元函数出发，构造了一类具备最优代数免疫的偶数元布尔函数，但是所构造的函数不平衡，而且非线性度也不高。付绍静等改进了Dalai的构造，使用迭代构造了一列达到最优代数免疫度的奇数元布尔函数。Dalai和付绍静的工作都是二阶递归构造，即由n元MAI函数构造$n+2$元MAI函数，陈银东等进一步给出了一个一阶递归构造，所构造的函数为平衡函数，并计算了他们的非线性度和代数次数[32]。

3.2 基于Reed Muller码生成矩阵构造最优代数免疫函数

3.2.1 引言

根据定理2.5可以知道，构造n元具备最优代数免疫布尔函数$f\left(wt(f)=s\right)$等价于找出式（2-13）中生成矩阵G的$s\times s$阶非奇异矩阵。更准确地说，根据式（3-6）对于一个正整数$1\le l\le s$，挑选两个向量子集：

$U=\{u_1,\cdots,u_t,u_{t+1},\cdots,u_l\}\subseteq W^{\ge k+1}$，$T=\{\beta_1,\cdots,\beta_t,\beta_{t+1},\cdots,\beta_l\}\subseteq W^{\le k}$，令$W^{\le k}\setminus T=\{\gamma_1,\gamma_2,\cdots,\gamma_{s-l}\}$。

根据基$\{c_{\beta_1},c_{\beta_2},\cdots,c_{\beta_l},c_{\gamma_1},c_{\gamma_2},\cdots,c_{\gamma_{s-l}}\}$，子矩阵$\left[c_{u_1},c_{u_2},\cdots,c_{u_l},c_{\gamma_1},c_{\gamma_2},\cdots,c_{\gamma_{s-l}}\right]$能表示成

$$\left[c_{u_1},c_{u_2},\cdots,c_{u_l},c_{\gamma_1},c_{\gamma_2},\cdots,c_{\gamma_{s-l}}\right]=\left[c_{\beta_1},c_{\beta_2},\cdots,c_{\beta_l},c_{\gamma_1},c_{\gamma_2},\cdots,c_{\gamma_{s-l}}\right]\begin{pmatrix}B & 0\\ C & I\end{pmatrix}$$

其中，B 是一个 $l\times l$ 阶分块矩阵，$B=\begin{pmatrix}A & 0\\ D & E\end{pmatrix}$，0 是零矩阵，$A=\left(a_{i,j}\right)$ 是一个 $t\times t$ 阶矩阵，$E=\left(e_{i,j}\right)$ 是一个 $(l-t)\times(l-t)$ 阶矩阵，I 是阶为 $s-l$ 的单位矩阵。因此，关键问题是找到两个向量子集 U 和 T 使得 B 是个可逆矩阵，进而推出矩阵 A,E 是可逆矩阵。

一般来说，矩阵 A,E 的秩是不容易确定的，但是如果 A,E 是一个上三角矩阵或者下三角矩阵，则很容易确定矩阵 A,E 的秩，从而可以判断 B 的秩。所以问题的关键是找到两个向量子集 $U=\{u_1,\cdots,u_t,u_{t+1},\cdots,u_l\}\subseteq W^{\geq k+1}$，$T=\{\beta_1,\cdots,\beta_t,\beta_{t+1},\cdots,\beta_l\}\subseteq W^{\leq k}$，满足下面的两个条件 C_1' 和 C_2'。

C_1'：在 c_{u_i} 的线性表示中 c_{β_i} 的系数是 1。等价于 $b_{i,j}=1\left(\beta_i\preceq u_i\right)$，$1\leq i\leq l$。

C_2'：在 c_{u_j} 的线性表示中 c_{β_i} 的系数是 0。等价于 $b_{i,j}=0\left(\beta_i\not\preceq u_j\right)$，当 $1\leq j<i\leq t$，或者 $1\leq i\leq t,\ t<j\leq l$，或者 $t<j<i\leq l$。

在这部分，将给出布尔函数 f 其支撑集 $\mathrm{supp}(f)=\left\{\left(W^{\leq k}\setminus T\right)\cup U\right\}$ 的新的构造方法，其中,向量 T,U 分别是从子集 $W^{\leq k}$ 和 $W^{\geq k+1}$ 中挑选出来的。同时给出了新构造的证明过程。

构造的主要思想是：在 Reed Muller 码生成矩阵 G 的一组基 $\left\{c_{\beta_1},\cdots,c_{\beta_l},c_{\gamma_1},\cdots,c_{\gamma_{s-l}}\right\}$ 下，首先用 t 个 c_{u_i} 且 $wt\left(u_i\right)=k+1$ 的向量替换 t 个 c_{β_i} 且 $wt\left(\beta_i\right)=1$ 的向量，用 $l-t$ 个 c_{u_i} 且 $wt\left(u_i\right)=k+m$（正整数 m 是满足 $\binom{k+m-2}{k-1}=0\left(\mathrm{mod}\,2\right)$ 的解）的向量替换 $l-t$ 个 c_{β_i} 且 $wt\left(\beta_i\right)=k$ 的向量，使得新的向量子集 $\left[c_{u_1},c_{u_2},\cdots,c_{u_l},c_{\gamma_1},c_{\gamma_2},\cdots,c_{\gamma_{s-l}}\right]$ 是 Reed Muller 码生成矩阵 G 的一组基。

3.2.2 代数免疫最优布尔函数的构造

设n为正整数，令$k=\lceil n/2\rceil-1$，$s=\sum_{i=0}^{k}\binom{n}{i}$，假定$\alpha_1,\alpha_2,\alpha_3,\cdots,\alpha_{2^n}$是$F_2$上的所有$n$维向量，他们是按照汉明重量和字典顺序排列的，即可以表示为

$\alpha_1=(0,0,0,0,\cdots,0)$ $\alpha_2=(1,0,0,0,\cdots,0)$, $\alpha_3=(0,1,0,0,\cdots,0),\cdots,\alpha_{n+1}=(0,0,0,0,\cdots,1)$,

$\alpha_{n+2}=(1,1,0,0,\cdots,0)$，$\alpha_{n+3}=(1,0,1,0,\cdots,0),\alpha_{n+4}=(1,0,0,1,\cdots,0),\cdots,\alpha_{\binom{n}{2}+n+1}=(000$

$\cdots11),\cdots,\alpha_{2^n}=(1,1,1,\cdots,1,1)$。则构造方法如下：

首先约定$\beta_j,u_j\in F_2^n,1\le j\le 2^n$，设向量子集$\{c_{\beta_1},c_{\beta_2},\cdots,c_{\beta_t},c_{\gamma_1},c_{\gamma_2},\cdots,c_{\gamma_{s-l}}\}$是 Reed Muller 码的生成矩阵$G$的一组基。

(1) 选取$T_1=\{\beta_1,\beta_2,\cdots,\beta_t\}$，且$wt(\beta_i)=p,1\le p\le k$，$1\le i\le t$。

(2) 选取$T_2=\{\beta_{t+1},\beta_{t+2},\cdots,\beta_l\}$，$wt(\beta_i)=k$，$t<i\le l$。令$W^{\le k}\setminus(T_1\cup T_2)=\{\gamma_1,\gamma_2,\cdots,\gamma_{s-l}\}$，$T=T_1\cup T_2$。

(3) 选取$U_1=\{u_1,u_2,\cdots,u_t\}$，$wt(u_i)=k+1$，$1\le i\le t$。

(4) 选取$U_2=\{u_{t+1},u_{t+2},\cdots,u_l\}$，$wt(u_i)=k+m$，$t<i\le l$且$1\le j\le n-k$，正整数$m$满足$\binom{k+m-1-p}{k-p}=0(\bmod 2)$且$(0\le m\le n-k)$，令$U=U_1\cup U_2$。

如果步骤(1),(2),(3),(4)均满足条件C_1'和C_2'且$0\le t\le\binom{n-k}{p}$，$0\le l-t\le\binom{n-m}{k}$等价于$0\le l\le\binom{n-m}{k}+\binom{n-k}{p}$。

则n元布尔函数f具有最优的代数免疫度，即$AI(f)=\left\lceil\frac{n}{2}\right\rceil$。其中，布尔函数等于 1 的自变量的集合是$\mathrm{supp}(f)=\{(W^{\le k}\setminus T)\cup U\}$。

如果n是奇数，则f是代数免疫最优的平衡布尔函数。

3.2.3 构造的证明

因为f的支撑集为$\mathrm{supp}(f)=\{(W^{\le k}\setminus T)\cup U\}$，说明用向量子集$U$替换了向量子集$T$，只需要证明$\left[c_{u_1},c_{u_2},\cdots,c_{u_l},c_{\gamma_1},c_{\gamma_2},\cdots,c_{\gamma_{s-l}}\right]$是$s\times s$阶的可逆矩阵。

首先根据式（3-7）有

$\left[c_{u_1},c_{u_2},\cdots,c_{u_l},c_{\gamma_1},c_{\gamma_2},\cdots,c_{\gamma_{s-l}}\right]=\left[c_{\beta_1},c_{\beta_2},\cdots,c_{\beta_l},c_{\gamma_1},c_{\gamma_2},\cdots,c_{\gamma_{s-l}}\right]\begin{pmatrix}B & 0\\ C & I\end{pmatrix}$，想要证明$\left[c_{u_1},c_{u_2},\cdots,c_{u_l},c_{\gamma_1},c_{\gamma_2},\cdots,c_{\gamma_{s-l}}\right]$是$s\times s$的可逆矩阵，由上式可知只需证明矩阵$\left[c_{\beta_1},\cdots,c_{\beta_l},c_{\gamma_1},\cdots,c_{\gamma_{s-l}}\right],\begin{pmatrix}B & 0\\ C & I\end{pmatrix}$是可逆矩阵即可。

因为$\{c_{\beta_1},c_{\beta_2},\cdots,c_{\beta_l},c_{\gamma_1},c_{\gamma_2},\cdots,c_{\gamma_{s-l}}\}$是Reed Muller码生成矩阵$G$的一组基，所以矩阵$\left[c_{\beta_1},c_{\beta_2},\cdots,c_{\beta_l},c_{\gamma_1},c_{\gamma_2},\cdots,c_{\gamma_{s-l}}\right]$是可逆矩阵，因此现在只需证明$\begin{pmatrix}B & 0\\ C & I\end{pmatrix}$是可逆矩阵，又由于矩阵是分块矩阵，则只需证明$B$是可逆矩阵。

现在令$B=\begin{pmatrix}A & H\\ D & E\end{pmatrix}$，其中$A=(a_{i,j})$是$t\times t$阶矩阵，$H=(h_{i,j})$是$t\times(l-t)$阶矩阵，$D=(d_{i,j})$是$(l-t)\times t$阶矩阵，$E=(e_{i,j})$是$(l-t)\times(l-t)$阶矩阵。

因为步骤(1)中的T_1和(2)中的T_2满足条件C_1'和C_2'，所以当$1\le i\le t$时，$a_{i,j}=1$，当$1\le j<i\le t$或者$(1\le i<j\le t)$时，$a_{i,j}=0$，因此$A=(a_{i,j})$是一个上三角矩阵或者下三角矩阵，即A是一个$t\times t$阶可逆矩阵。

根据步骤(4)可知，m是满足$\binom{k+m-2}{k-1}=0(\mathrm{mod}\,2)$的解，且又有$wt(c_{u_j})=k+m$，所以$wt(\beta_r)=k-k+1=1$，得到在$c_{u_j}\ (t<j\le l)$的线性表示式中$c_{\beta_i}$的系数为0，$1\le i\le t$。

则根据定理 2-7 可知 $a_{k-1}^{(m)}=h_{i,j}=0$，$t<j\le l$，所以可以得到矩阵 $H=\left(h_{i,j}\right)$ 是一个 $t\times(l-t)$ 阶 0 矩阵。

因为步骤 (2) 和步骤 (4) 满足条件 C_1' 和 C_2'，则当 $t<i\le$ 时，$e_{i,j}=1$，当 $t\le j<i\le(t\le i<j\le$ 时，$e_{i,j}=0$。所以矩阵 $E=\left(e_{i,j}\right)$ 是一个上三角矩阵或者下三角矩阵，即 E 是一个 $(l-t)\times(l-t)$ 阶可逆矩阵。

因为 $B=\begin{pmatrix}A & H\\ D & E\end{pmatrix}$，$A,E$ 是可逆矩阵，H 是 0 矩阵，即分块矩阵 B 是一个 $l\times l$ 阶可逆矩阵。所以分块矩阵 $\begin{pmatrix}B & 0\\ C & I\end{pmatrix}$ 是一个 $s\times s$ 的可逆矩阵。则

$$\left[c_{u_1},c_{u_2},\cdots,c_{u_l},c_{\gamma_1},c_{\gamma_2},\cdots,c_{\gamma_{s-l}}\right]=\left[c_{\beta_1},c_{\beta_2},\cdots,c_{\beta_l},c_{\gamma_1},c_{\gamma_2},\cdots,c_{\gamma_{s-l}}\right]\begin{pmatrix}B & 0\\ C & I\end{pmatrix}$$

是一个 $s\times s$ 的可逆矩阵。

接下来证明 t 和 l 的取值范围

因为用向量子集 $U_1=\{u_1,u_2,\cdots,u_t\}$ 替换了向量子集 $T_1=\{\beta_1,\beta_2,\cdots,\beta_t\}$，矩阵 A 是可逆矩阵。又因为 $wt(u_i)=k+1$，所以 c_{u_i} 的线性表示中至少有 $k+1$ 个 c_{β_j}，因此至多有 $n-k$ 个向量线性无关，即 $t\le\binom{n-k}{p}$。

由于用向量子集 $U_2=\{u_{t+1},u_{t+2},\cdots,u_l\}$ 替换了向量子集 $T_2=\{\beta_{t+1},\beta_{t+2},\cdots,\beta_l\}$，因为 $wt(u_j)=k+m$，若 $u_{t+1}=1\cdots10\cdots0$，有 $k+m$ 个 1，则 $c_{u_{t+1}}$ 的线性表示中 $c_{\beta_i}\ (t<i\le l)$ 的最大的 i 的取值是使得 $\beta_i=00\cdots011\cdots10\cdots0$，其中有 k 个 1，1 前面有 m 个 0，如果要使 $l-t$ 个 $c_{u_j}\ (t<j\le l)$ 线性无关，则 $l-t\le\binom{n-m}{k}$，因此 $l\le\binom{n-m}{k}+\binom{n-k}{p}$。

于是函数值等于 1 的自变量的集合为 $\mathrm{supp}(f)=\left\{\left(W^{\le k}\setminus T\right)\cup U\right\}$ 的 n 元布尔函数 f 具备最优的代数免疫度，即 $AI(f)=\left\lceil\frac{n}{2}\right\rceil$。

如果 n 为奇数，因为 $\sum_{i=0}^{n}\binom{n}{i}=\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{n}=2^n$，总共有 $n+1$ 项，而且为偶数，$k=\left\lceil\frac{n}{2}\right\rceil-1=\frac{n-1}{2}$，$s=\sum_{i=0}^{k}\binom{n}{i}$，其中总共有 $\frac{n+1}{2}$，所以 $2\sum_{i=0}^{k}\binom{n}{i}=2^n$，即 $s=2^{n-1}$，所以奇变元布尔函数 f 是具有最优代数免疫的平衡函数。

假如 n 为偶数，则 $s=\sum_{i=0}^{k}\binom{n}{i}=2^{n-1}-\binom{n}{n/2}$，则真值表中 0 比 1 的数目多 $\binom{n}{n/2}$ 个，于是需要我们把函数真值表中 $\binom{n}{n/2}$ 个 0 改为 1，修改后的布尔函数是代数免疫最优的均衡函数。

接下来用一个 n 是奇数的例子对上述的构造方法进行说明。

例 令 $n=9$，$k=\left\lceil\frac{n}{2}\right\rceil-1=\left\lceil\frac{9}{2}\right\rceil-1=4$，$s=\sum_{i=0}^{k}\binom{n}{i}=\sum_{i=0}^{2}\binom{9}{i}=2^{n-1}=2^8=256$，$p=1$，$t=\binom{n-k}{p}=\binom{9-4}{1}=5$，因为 $\binom{k+m-1-p}{k-p}=\binom{m+2}{3}=0(\mathrm{mod}\,2)$，所以 m 可能的取值为 2，3，4，现在令 $m=4$，$l=\binom{n-m}{k}+\binom{n-k}{p}=\binom{9-4}{4}+\binom{5}{1}=10$。

约定 F_2^9 上的所有 9 维向量按照汉明重量和字典顺序排列，即表示 $\alpha_1=000000000$，$\alpha_2=100000000$，$\alpha_3=010000000$，α_4=001000000，…，α_{10}=000000001，$\alpha_{11}=11000$ 0000，α_{12}=101000000，…，α_{46}=000000011，…，α_{511}=011111111，α_{512}=1111111，11，令 $V=W^{\le 4}\setminus\left(T_1\cup T_2\right)=\left\{\gamma_1,\gamma_2,\cdots,\gamma_{10}\right\}$。

现在构造$T=T_1\cup T_2, U=U_1\cup U_2$：

$T_1=\{\beta_1,\beta_2,\beta_3,\beta_4,\beta_5\}$，设$\beta_1$=$\alpha_6$=000010000，$\beta_2$=$\alpha_7$=000001000，$\beta_3$=$\alpha_8$=00000 0100，$\beta_4=\alpha_9=000000010$，$\beta_5=\alpha_{10}=000000001$。$U_1$=$\{u_1,u_2,u_3,u_4,u_5\}$，且每个向量的重量为 5，$u_1=\alpha_{257}=111110000$，$u_2=\alpha_{262}=111011000$，$u_3=\alpha_{266}$=111001100，$u_4=\alpha_{285}=110010110$，$u_5=\alpha_{382}=000011111$。根据条件$C_1^{'}$和$C_2^{'}$，在$c_{u_1}$的线性表示中只有$c_{\beta_1}$，则$a_{1,1}=1$，$a_{2,1}$=0，$a_{3,1}=0,a_{4,1}=0,a_{5,1}=0$，$c_{u_2}$的线性表示中只有$c_{\beta_1},c_{\beta_2}$，则$a_{1,2}=a_{2,2}=1,a_{3,2}=a_{4,2}=a_{5,2}=0$，以此类推，$a_{2,3}=a_{3,3}=1,a_{1,3}=a_{4,3}=a_{5,3}=0$，$a_{1,4}=a_{3,4}=a_{4,4}=1,a_{2,4}=a_{5,4}=0$，$a_{1,5}=a_{2,5}=a_{3,5}=a_{4,5}=a_{5,5}=1$，所以

$$A=\begin{pmatrix}1&1&0&1&1\\0&1&1&0&1\\0&0&1&1&1\\0&0&0&1&1\\0&0&0&0&1\end{pmatrix}$$

是一个上三角矩阵。

我们规定$T_2=\{u_{5+1},u_{5+2},\cdots,u_{10}\}$，其中每个向量分别为$\beta_6$=$\alpha_{252}$=000011110，$\beta_7$=$\alpha_{253}$=000011101，$\beta_8$=$\alpha_{254}$=000011011，$\beta_9$=$\alpha_{255}$=000010111，$\beta_{10}$=$\alpha_{256}$=000001111。$U_2=\{u_{5+1},u_{5+2},\cdots,u_{10}\}$，其中每个向量的汉明重量为 8，即有$u_6=\alpha_{503}=111111110$，$u_7=\alpha_{504}=111111101$，$u_9=\alpha_{506}=111110111$，$u_{10}=\alpha_{508}=111011111$，根据条件$C_1^{'}$和$C_2^{'}$，有$e_{6,6}=1,e_{7,6}=e_{8,6}=e_{9,6}=e_{10,6}=0$，$e_{7,7}=1,e_{6,7}=e_{8,7}=e_{9,7}=e_{10,7}=0$，$e_{8,8}=1,e_{6,8}=e_{7,8}=e_{9,8}=e_{10,8}=0$，$e_{9,9}=1,e_{6,9}=e_{7,9}=e_{8,9}=e_{10,9}=0$，$e_{6,10}=e_{7,10}=e_{8,10}=e_{9,10}=e_{10,10}=1$，所以矩阵

$$E=\begin{pmatrix}1&0&0&0&1\\0&1&0&0&1\\0&0&1&0&1\\0&0&0&0&1\\0&0&0&1&1\end{pmatrix}$$

是一个上三角矩阵。

因为U_2中的每一个向量$u_j\left(5\le j\le 10\right)$的汉明重量为$4+m$，又因为$m=4$，所以，$c_{u_j}$的线性表示中$c_{\beta_i}\left(1\le i\le 5\right)$（且每一个$\beta_i$的汉明重量都为 1）系数都为 0，是因为$h_{i,j}=\binom{m+2}{3}=\binom{6}{3}=0\left(\mathrm{mod}\,2\right)$，因此矩阵$H$是一个 0 矩阵。由此可以看出矩阵$\left[c_{u_1},\cdots,c_{u_{10}},c_{\gamma_1},\cdots,c_{\gamma_{246}}\right]$是一个 256*256 阶的可逆矩阵，于是支撑集是$\mathrm{supp}\left(f\right)=\left\{\left(W^{\le 4}\setminus T\right)\cup U\right\}$的 9 元布尔函数$f$具备最优的代数免疫度，即$AI\left(f\right)=\left\lceil\frac{n}{2}\right\rceil=5$。

3.2.4 具有最优代数免疫的一阶弹性布尔函数

上一节中主要应用 Reed Muller 码的生成矩阵构造出了代数免疫度最优的平衡布尔函数。这部分最主要是建立在上一节的基础上，对它进一步优化，使其成为具备最优代数免疫的一阶弹性布尔函数，能够更好地抵御所有已知攻击。

下面首先给出构造相关免疫函数的标准方法[33],它被称为 LT 方法。

一个n维布尔函数$f\in B_n$，定义S_f是一个$W_f\left(\omega\right)=0$的所有ω的向量集合。其中，W_f是布尔函数f的*walsh*谱。

若是S_f中存在n个线性无关的向量，找出一个$n\times n$阶可逆矩阵B_f，它的行向量是S_f中n个线性无关的的向量。令$C_f=B_f^{-1}$，现在构造一个布尔函数$f'\left(X\right)=f\left(C_fX\right)$，则$f',f$具备一样的非线性度和代数次数，而且在$wt\left(\omega\right)=1$时，有

$W_{f'}(\omega)=0$，于是 f' 是一阶相关免疫布尔函数，同理，如果 f 是均衡的，则 f' 也是均衡的，即 f' 是一阶弹性布尔函数。

现在对上一节的构造进行改进，使其成为具有最优代数免疫的一阶弹性布尔函数。

改进的步骤如下：

f 是上一节构造的 n 维布尔函数，支撑集为 $\mathrm{supp}(f)=\left\{\left(W^{\le k}\setminus T\right)\cup U\right\}$，$T,U$ 是构造中给出的。

(1) 首先根据布尔函数的 *walsh* 谱公式 $W_f(\omega)=\sum_{x\in \mathrm{F}_2^n}(-1)^{f(x)+x\cdot\omega},\omega\in \mathrm{F}_2^n$，计算出布尔函数 f 在 F_2^n 上每个点 ω 处的 *walsh* 谱值。

(2) 在所有 *walsh* 谱值为 0（$S_f=\left\{\omega\in\{0,1\}^n \mid W_f(\omega)=0\right\}$）的向量中找出 n 个向量，如果它们是线性无关的，则可构成可逆矩阵 B_f，如果不存在，则布尔函数 f 不能修改成一阶弹性函数。

(3) 如果存在这样的可逆矩阵 B_f，则编程计算可逆矩阵 B_f 的逆矩阵 $C_f=B_f^{-1}$，然后构造 n 维布尔函数 g，使得 $g(X)=f(C_fX)$,其中，$X=(x_1,x_2,\cdots,x_n)$，则布尔函数 g 和布尔函数 f 具有相同的非线性度，代数次数，代数免疫度，且在每个汉明重量为 1 的向量 $x\in \mathrm{F}_2^n$ 处的 *walsh* 谱值为 0，又有 g 是平衡函数，所以根据定理 2-2 的 Xiao-Massey 定理，对于向量 $\omega\in \mathrm{F}_2^n$, 当 $0\le wt(\omega)\le 1$ 时，有 $W_g(\omega)=0$，于是 g 是满足代数免疫最优且具备一阶弹性的函数。

3.3 本章小结

本章首先给出了几种常用的代数免疫最优布尔函数的构造方法，接下来根据 Sihong su 的论文[27]，给出了一种基于 Reed Muller 码生成矩阵构造代数免疫最优布尔函数的方法，并给出了简单的证明，同时在 n=9 时，给出了代数免疫最优布尔函数

的一个实例对其给予说明。最后在这个构造的基础上对其进行了一些修改和改进，使其具有一阶弹性，从而能够更好地抵抗各种已知的密码攻击。

本章给出的一种构造最优代数免疫的布尔函数的方法，但是同时也遗留一些问题有待去进一步的研究，例如：

虽然布尔函数的代数免疫达到了最优且具有一阶弹性，但是因为此构造是在 MAI 函数的基础上进行了仿射变换，所以其非线性度的下界是 MAI 函数的下界，非线性度比较差。因此还需要进一步的研究和讨论，从而能够提出一种有效的方法，使得各种密码指标都尽可能的好。

第四章 M-M 类函数和部分 PS 类函数的性能分析

4.1 M-M 构造和 PS 构造

作为密码函数，Bent 函数具备比较明显的优点，首先，它具备最优的 N_f，因此，它能够很好地抵抗线性攻击和最佳仿射逼近攻击，其次，它具有完全非线性性，因此它是抵抗差分密码攻击的最优函数，最后，Bent 函数 Walsh 谱在每一点的取值为 $\pm 2^{n/2}$，根据流密码的稳定性理论，以 Bent 函数为非线性组合函数和滤波函数的秘钥流序列具有稳定的线性复杂度，所以 Bent 函数的构造是 Bent 函数研究中的热点问题。代表性的方法有 M-M 构造和 PS 构造。

下面，首先给出 Bent 函数的相关概念[21]。

定理 4.1 设 $f(x)$ 是 n 元布尔函数，则布尔函数 $f(x)$ 是 Bent 函数的充要条件是对任意自变量 $a \in \mathrm{F}_2^n$，$W_f(a)$ 的取值只能是 $\pm 2^{n/2}$。

根据 Bent 函数的定义，我们知道它的非线性度为 $N_f = 2^{n-1} - 2^{\frac{n}{2}-1}$，所以进一步可以得到 $\max\limits_{\omega \in \mathrm{F}_2^n} \left| W_f(\omega) \right| = 2^{\frac{n}{2}}$，$\sum\limits_{\omega \in \mathrm{F}_2^n} W_f^2(\omega) \le 2^n \cdot 2^n = 2^{2n}$，又因为定理 2-1（Parseval 恒等式），所以 W_f 只能是 $\pm 2^{\frac{n}{2}}$。

接下来给出第一个直接构造 Bent 函数的方法，即 Maiorana-McFarland 构造法，简称 M-M 构造法。

定义 4.2 设 n 为偶数，$\mathrm{F}_2^n = \left\{ (x,y) \mid x,y \in \mathrm{F}_2^{\frac{n}{2}} \right\}$，$\mathrm{F}_2^n$ 上的 Maiorana-McFarland 型布尔函数简称为 M-M 型函数[15][32]，定义为 F_2^n 上所有线性函数或仿射函数的级联，也可以表示为所有线性函数或仿射函数的真值表的排列。

定理 4.2 设 f 是 F_2^n 上的 M-M 型函数，则 f 是 Bent 函数。

证明 由于 f 为 F_2^n 上的 M-M 型函数，则布尔函数 f 可以表示为式的形式，所以有下式成立

$$\begin{aligned} W_f(a,b) &= \sum_{x\in \mathrm{F}_2^{n/2}} \sum_{y\in \mathrm{F}_2^{n/2}} (-1)^{x\cdot\pi(y)+g(y)+a\cdot x+b\cdot y} \\ &= \sum_{y\in \mathrm{F}_2^{n/2}} (-1)^{b\cdot y+g(y)} \sum_{x\in \mathrm{F}_2^{n/2}} (-1)^{x\cdot(a+\pi(y))} \\ &= 2^{n/2}(-1)^{b\cdot\pi^{-1}(a)+g(\pi^{-1}(a))} \\ &= \pm 2^{n/2} \end{aligned}$$

故布尔函数 f 是 Bent 函数。

接下来，介绍另一种直接构造 Bent 函数的方法，该方法是 Dillon 在他的博士论文[35]中给出的。

定义 4.3 设 E 是 F_2^n 的一个线性子空间，E 的指标函数定义为

$$1_E = \begin{cases} 1, x \in E \\ 0, x \notin E \end{cases} \tag{4-1}$$

如果 E_1 和 E_2 是 F_2^n 上的两个线性子空间，并且 $E_1 \cap E_2 = \{0\}$，那么称线性子空间 E_1 和 E_2 是不相交的。

引理 4.1 当 n 为偶数时，F_2^n 中两两不相交的 $\frac{n}{2}$ 维线性子空间恰有 $2^{\frac{n}{2}}+1$ 个。

证明 设在 F_2^n 中两两不相交的 $\frac{n}{2}$ 维线性子空间一共有 k 个，则可以得到下面的两个式子

$$2^n - k\left(2^{\frac{n}{2}}-1\right) \geq 1$$

$$k \leq \left[\frac{2^n-1}{2^{\frac{n}{2}}-1}\right] = 2^{\frac{n}{2}}+1$$

上式表明 F_2^n 中两两不相交的 $\frac{n}{2}$ 维线性子空间至多有 $2^{\frac{n}{2}}+1$ 个。

注意下面 $2^{n/2}+1$ 个子空间的维数均是 $\frac{n}{2}$ 而且两两向量空间是不相交的，$V_0 = \{(x,0) \mid x \in \mathrm{F}_2^{n/2}\}$，$V_a = \{(ay,y) \mid y \in \mathrm{F}_2^{n/2}\}, a \in (\mathrm{F}_2^{n/2})^*$，其中，$ay$ 是 $\mathrm{F}_2^{n/2} \to \mathrm{F}_2^{n/2}$ 中的乘法运算。于是，F_2^n 中两两不相交的 $\frac{n}{2}$ 维线性子空间恰有 $2^{n/2}+1$ 个。

为了给出直接构造 Bent 函数的方法，Dillon 引进了局部扩散（Partial Spread）类的概念，简称为 PS 类。F_2^n 上的 PS 类函数是指由 F_2^n 中任意 $2^{n/2-1}$ 个或者 $2^{n/2-1}+1$ 个互不相交的 $\frac{n}{2}$ 维线性子空间的指标函数模 2 和所组成的函数的集合，分别用 PS^- 和 PS^+ 来表示。

定理 4.3 *PS* 类函数是 Bent 函数。

证明 下面只给出 PS^- 类函数为 Bent 函数的证明，PS^+ 类函数的证明类似。

设 $E_0, E_1, \cdots, E_{2^{n/2}}$ 是 F_2^n 中 $2^{\frac{n}{2}}+1$ 个互不相交的 $\frac{n}{2}$ 维线性子空间，不失一般性，可以假设

$$f(x) \equiv \sum_{i=0}^{2^{\frac{n}{2}-1}-1} 1_{E_i}(x) \bmod 2 \tag{4-2}$$

所以，对任意 $a \in F_2^n$，都有

$$\begin{aligned} W_f(a) &= \sum_{a \in F_2^n} (-1)^{f(x)+a\cdot x} \\ &= \sum_{i=0}^{2^{\frac{n}{2}-1}-1} \sum_{x \in E_i} (-1)^{1+a\cdot x} + \sum_{i=2^{\frac{n}{2}-1}}^{2^{\frac{n}{2}}} \sum_{x \in E_i} (-1)^{0+a\cdot x} \\ &= \sum_{i=2^{\frac{n}{2}-1}}^{2^{\frac{n}{2}}} \sum_{x \in E_i} (-1)^{a\cdot x} - \sum_{i=0}^{2^{\frac{n}{2}-1}-1} \sum_{x \in E_i} (-1)^{a\cdot x} \end{aligned}$$

如果 $a=0$ 时，则 $W_f(a)=2^{\frac{n}{2}}$；如果 $a \neq 0$ 时，由于这 $2^{\frac{n}{2}}+1$ 个线性子空间的对偶空间 $E_i^{\perp}$ 任然是互不相交的线性子空间，所以 a 一定属于且只属于这些对偶子空间的某一个子空间，并且记为 $E_j^{\perp}$，此时就有

$$\sum_{x \in E_i} (-1)^{u\cdot x} = \begin{cases} 2^{\frac{n}{2}}, & i=j \\ 0, & i \neq j \end{cases} \tag{4-3}$$

于是就可以得到 $W_f(a) = \pm 2^{\frac{n}{2}}$，所以 PS^- 类函数是 Bent 函数。

4.2 M-M 类和 PS 类布尔函数的性能分析

这一节主要是修改 M-M 类函数和 PS 类函数，然后对它们的非线性度和代数免疫度进行分析和研究，并给出相关的结论。

I M-M 构造

由上一节式（4-1）可知构造 M-M 类函数的实质就是：级联 $2^{\frac{n}{2}}$ 个 $\frac{n}{2}$ 元线性布尔函数（或仿射函数），使其成为一个 n（n 为偶数）元 Bent 函数，也就是说把 $2^{\frac{n}{2}}$ 个 $\frac{n}{2}$ 元线性布尔函数的真值表排起来，构成一个 2^n 长的真值表，并且其非线性度为达到最优为 $2^{n-1}-2^{\frac{n}{2}-1}$。

由 Bent 函数的定义可知，其在 F_2^n 中的每一点上的 *walsh* 谱值为 $\pm 2^{\frac{n}{2}}$，因为平衡函数在全 0 点的 *walsh* 谱值为 0，所以 Bent 函数不是平衡函数。

II PS 构造

根据第一节对 PS 构造的介绍，可以知道，构造 PS 类函数的关键是在 F_2^n 找到 $2^{\frac{n}{2}}+1$ 个互不相交的 $\frac{n}{2}$ 维线性子空间。下面给出互不相交线性子空间的构造。

首先，把向量空间 $F_2^{\frac{n}{2}}$ 对应到有限域 $F_{2^{n/2}}$ 上，令 $m(x)$ 为域 $F_{2^{n/2}}$ 上的 n 次本原多项式，假设 n 维初始向量为 a_0 且不等于全 0 向量，用线性反馈移位寄存器生成 m 序列，把连续 n 个向量记为 a_i，则 m 序列可以生成除全 0 外，整个向量空间且 $0 \le i \le 2^{\frac{n}{2}}-2$，再加上全 0 向量则可构成 n 维向量空间，令 $E_0, E_1, E_2, \cdots, E_{2^{n/2}}$ 是 F_2^n 中 $2^{\frac{n}{2}}+1$ 个互不相交的 $\frac{n}{2}$ 维线性子空间，$G_0, G_1, G_2, \cdots, G_{2^{n/2}}$ 是 $E_0, E_1, E_2, \cdots, E_{2^{n/2}}$ 的生成矩阵，G_i 可以表示成以下的形式

$$G_0=\left(I\left|\begin{matrix}a_0\\a_1\\\vdots\\a_{n/2-1}\end{matrix}\right.\right),\quad G_2=\left(I\left|\begin{matrix}a_1\\a_2\\\vdots\\a_{n/2}\end{matrix}\right.\right),\quad G_3=\left(I\left|\begin{matrix}a_2\\a_3\\\vdots\\a_{n/2+1}\end{matrix}\right.\right),\quad \cdots,\quad G_{2^{n/2}-2}=\left(I\left|\begin{matrix}a_{2^{n/2}-2}\\a_0\\\vdots\\a_{n/2-2}\end{matrix}\right.\right),$$

$$G_{2^{n/2}-1}=(I|0),\quad G_{2^{n/2}}=(0|I) \tag{4-4}$$

其中，I 是 $\frac{n}{2}\times\frac{n}{2}$ 阶单位矩阵，0 是 $\frac{n}{2}\times\frac{n}{2}$ 阶零矩阵。则由 $G_0,G_1,G_2,\cdots,G_{2^{n/2}}$ 生成的向量子空间 $E_0,E_1,E_2,\cdots,E_{2^{n/2}}$ 是不相交的，这是因为每个生成矩阵中的行向量与其他生成矩阵中的行向量是线性无关的。

接下来在这 $2^{\frac{n}{2}}+1$ 个不相交子空间中任意挑选 $2^{\frac{n}{2}-1}$ 个子空间，使其成为布尔函数 $f\in B_n$ 的支撑集，记为 supp(f)，则构造的布尔函数是 PS 类 Bent 函数，其非线性度达到最优。

按照定理 4.10 的方法，构造的 Bent 函数是一类特殊的 PS$^-$函数，称之为 PS_{ap} 函数。PS_{ap} 函数具有以下的明确的表达式

$$f(x,y)=\begin{cases}0, & y=0\\ g\left(\frac{x}{y}\right), & y\neq 0\end{cases} \tag{4-5}$$

其中，$x,y\in F_2^{\frac{n}{2}}$，g 为 $\frac{n}{2}$ 元平衡布尔函数且满足 $g(0)=0$。

下面介绍的 PS 类函数都是 PS_{ap} 函数。

虽然 Bent 函数的非线性度达到最优，能够很好地抵抗线性攻击，但其也有明显的缺点，根据 Bent 函数的定义可知，其在 F_2^n 上的每一点的 walsh 谱值只为 $\pm 2^{\frac{n}{2}}$，于是 Bent 函数不是均衡布尔函数，而且是相关免疫为 0。

III M-M 类和 PS 类平衡函数非线性度和代数免疫的比较

平衡函数修改的主要思想[35]：如果 n 元布尔函数 $f(x),x\in F_2^n$，是由 $2^{\frac{n}{2}}$ 个 $\frac{n}{2}$ 元线性布尔函数级联而成的布尔函数，即 M-M 类函数或者是由 $2^{\frac{n}{2}}+1$ 个 $\frac{n}{2}$ 维不相交子空间构造的布尔函数，即 PS 类函数，则其真值表中 0 比 1 的个数多 $2^{\frac{n}{2}}$ 个，如果想使布尔函数 f 是平衡函数则必须把真值表中 $2^{\frac{n}{2}-1}$ 个 0 改成 1。其结果是非线性度至多减少

$2\cdot 2^{\frac{n}{2}-1}=2^{\frac{n}{2}}$，给出非线性度的下界，即非线性度为 $N_f \geq 2^{n-1}-2^{\frac{n}{2}}$，然而在有些构造中非线性度是严格大于 $2^{n-1}-2^{\frac{n}{2}}$ 的。

下面给出非线性度的证明过程：

证明 设 n 元布尔函数 $f(x)\in B_n$ 是 M-M 类 Bent 函数或者是 PS 类 Bent 函数。假设另一个布尔函数 $g(x)\in B_n$，现在假设只修改了其中的 1 个比特，即把真值表中一个 0 改成了 1。

约定布尔函数 $g(x)$ 为：当 $x\neq k$ 时，$g(x)=f(x)$；当 $x=k$，$f(x)=0$ 时，$g(x)=1$。

则根据 walsh 谱的定义（式 2-7）可以得到，对于任意的 $\omega\in \mathrm{F}_2^n$，都有

$$\begin{aligned}W_g(\omega)&=\sum_{x\in \mathrm{F}_2^n}(-1)^{g(x)+x\cdot\omega}\\&=\left|\left\{x\mid g(x)=x\cdot\omega,x\in \mathrm{F}_2^n\right\}\right|-\left|\left\{x\mid g(x)\neq x\cdot\omega,x\in \mathrm{F}_2^n\right\}\right|\\&=\left|\left\{x\mid f(x)=x\cdot\omega,x\in \mathrm{F}_2^n,x\neq k\right\}\right|-\left|\left\{x\mid f(x)\neq x\cdot\omega,x\in \mathrm{F}_2^n,x\neq k\right\}\right|+(-1)^{-1+k\cdot\omega}\\&=W_f+2\cdot(-1)^{-1+k\cdot\omega}\end{aligned}$$

其中，$|A|$ 代表集合 A 中元素的个数。

所以布尔函数 g 在 ω 处的 walsh 谱也可以表示成布尔函数 g 和线性函数 $\omega\cdot x$ 相等的自变量的个数减去不相等的自变量个数。

下面分两种情况进行讨论

如果对于 n 维向量 $k\in\left\{x\mid f(x)\neq x\cdot\omega,x\in \mathrm{F}_2^n\right\}$，并且有 $f(k)=0$，如果现在把 k 的函数值从 0 改成 1，即有 $f(k)=1$，则可以得到 $f(k)\neq k\cdot\omega$，进而可以得到 n 维向量 $k\in\left\{x\mid f(x)\neq x\cdot\omega,x\in \mathrm{F}_2^n\right\}$，因此集合 $\left|\left\{x\mid f(x)=x\cdot\omega,x\in \mathrm{F}_2^n\right\}\right|$ 中元素的个数减 1，而集合 $\left|\left\{x\mid f(x)\neq x\cdot\omega,x\in \mathrm{F}_2^n\right\}\right|$ 中元素的个数加 1，所以布尔函数 f 在 ω 处的 walsh 谱加-2。所以布尔函数 g 在 ω 处的 walsh 谱等于布尔函数 f 在 ω 处的 walsh 谱加-2。

同理，如果对于自变量 $k\in\left\{x\mid f(x)\neq x\cdot\omega,x\in \mathrm{F}_2^n\right\}$，且有 $f(k)=0$，现在把 k 的函数值从 0 改成 1，即有 $f(k)=1$，则会得到 $f(k)=k\cdot\omega$，所以 $k\in\left\{x\mid f(x)=x\cdot\omega,x\in \mathrm{F}_2^n\right\}$，

因此集合$\left|\left\{x \mid f(x)=x\cdot\omega, x\in \mathrm{F}_2^n\right\}\right|$中元素的个数加 1，而集合$\left|\left\{x \mid f(x)\neq x\cdot\omega, x\in \mathrm{F}_2^n\right\}\right|$中元素的个数减 1，所以布尔函数 f 在 ω 处的 walsh 谱加 2，所以布尔函数 g 在 ω 处的 walsh 谱等于布尔函数 f 在 ω 处的 walsh 谱值加 2。

于是，若是修改函数真值表中的 1 比特，布尔函数的 walsh 谱值或者加上 2 或者减去 2，即增加 ±2。

进一步如果现在对布尔函数 f 真值表中 $2^{\frac{n}{2}-1}$ 个值进行修改，即把 $2^{\frac{n}{2}-1}$ 个 0 变成 1，则平衡布尔函数 f 在 F_2^n 上的每一点处的 walsh 谱值将会是 $W_f\overbrace{\pm 2\pm 2\pm 2\cdots+2}^{2^{\frac{n}{2}-1}}$。所以最坏的情况下，walsh 谱值会在 Bent 函数 walsh 谱值的基础上减少 $2\cdot 2^{\frac{n}{2}-1}=2^{\frac{n}{2}}$，因此可以得到布尔函数 f 非线性度的下界为 $2^{n-1}-2^{\frac{n}{2}-1}-\frac{1}{2}\cdot 2^{\frac{n}{2}-1}=2^{n-1}-2^{\frac{n}{2}}$，所以修改后的布尔函数的非线性度为 $N_f\geq 2^{n-1}-2^{\frac{n}{2}}$。

通过对两种功能函数的分析可以得到以下的结论：修改 M-M 类函数构造一类具备高非线性度、最优代数免疫的弹性函数是很困难的。只可举出部分例子，比如在论文附录 I 中给出的 n=8,10,12 时的函数。因为 PS 类函数具备比较好的代数结构，所以能够构造出一类具备高非线性度，代数免疫最优的均衡函数。函数我们可以阅读下面的论文 [19] (A Conjecture on Binary String and Its Applications on Constructing Boolean function of Optimal Algebraic Immunity)。

下面给出经过修正 M-M 类函数得到具备高非线性度,代数免疫最优的布尔函数，(8,0,6,112,3)，(8,1,6,112,3)，(10,0,8,472,4)，(10,1,8,472,4)，(10,0,8,482,4) (12,0,10,1984,5)。其中，(n,m,d,N_f,AI) 表示布尔函数的各个性质，n 表示变元个数，m 表示弹性阶，d 表示代数次数，N_f 表示非线性度，AI 表示代数免疫度。具体真值表可以参见附录 A(A1-A4)。

4.3 本章小结

本章最初给出了 Bent 函数的定义，并介绍了构造 Bent 函数的两种直接方法，M-M 构造和 PS 构造。在第二小节中给出了 PS 构造中 $2^{\frac{n}{2}}+1$ 个不相交子空间的构造方法。虽然 Bent 函数达到了非线性度最优，但其却不能满足密码函数的密码指标平衡性，所以接下来介绍了 M-M 类和 PS 类平衡函数，其主要思想是通过把真值表中 $2^{\frac{n}{2}-1}$ 个等于 0 的值改成 1，从而使其达到平衡，进而得出平衡布尔函数的非线性度至多减少 $2^{\frac{n}{2}-1}$，并对其进行了证明。

通过分析两类函数可以得到以下的结论：通过分析得到了以下结论：M-M 函数很难通过修改真值表得到一类高非线性度、代数免疫最优的弹性函数或平衡函数。只能给出一些例子，如附录 I 中给出 n=8,10,12 时，几个代数免疫最优，高非线性度的函数。而现在已知的 M-M 类函数不是代数免疫度最优的。可参见 Zhang 论文中的构造函数[37]。PS_{ap} 函数因为有好的代数结构，都可以修改成高非线性度，代数免疫最优的布尔函数。

本章的工作还存在一些不足之处，需要进一步的讨论和研究，虽然在 n=8,10,12 时，给出了具备高非线性度，代数免疫最优的 M-M 类布尔函数，但没有给出具体的构造方法。

第五章 总结与展望

作为流密码和分组密码算法重要组成部件的布尔函数，其密码性质的好与坏直接影响到密码体系的安全性。所以，在流密码和分组密码中，人们需要寻求具有各种密码学性质的布尔函数来构造密码算法，以抵抗多年来相继出现的各种攻击（差分密码攻击，线性密码攻击，相关攻击和代数攻击等）。本文主要对一类具备代数免疫最优布尔函数的新方法进行了阐述，而且 M-M 类和 PS 类函数进行了分析，得出了一些相关的结论，取得的主要成果有：

1. 结合 Sihong Su 和 Xiaohu Tang[27]的构造，给出了构造具备最优代数免疫度的布尔函数的新方法，并证明其代数免疫度是达到最优，并通过数据对其结果进行了说明，最后运用 LT 方法把具有最优代数免疫的布尔函数变换成一阶弹性函数。

2. 首先介绍了 M-M 类和 PS 类 Bent 函数和把其修改成平衡函数的方法，并给出了非线性度的下界和证明。通过分析两类函数可以得到以下的结论：通过分析两类函数，可以得到以下的结论：通过分析得到了以下结论：只有在限制一些条件的情况下，才可以构造出具备高非线性度、代数免疫最优的布尔函数。而现在已知的 M-M 函数中大多数不是代数免疫最优的。PS_{ap} 函数因为有好的代数结构，都可以修改成高非线性度，代数免疫最优的布尔函数。下面列出作者将要研究和深入研究的方向：

非线性度仍然是构造布尔函数最终主要的指标之一，是现在密码学者研究的热点问题，如何构造高非线性度且最优代数免疫度的布尔函数仍然需要进一步的研究与讨论；

由于作者水平有限，论文中还存在着一些不足之处，希望可以得到各位评审专家和读者批评指正。

致 谢

时光飞逝，岁月如梭，转眼间两年半的研究生生活即将告一段落，回顾这两年来的学习经历，还历历在目，在这期间我得到了很多人的帮助和鼓励。

首先由衷的感谢我的导师张卫国副教授！本论文的研究工作是在他的悉心的指导下完成的，这篇论文凝聚了张老师对我的精心培养和教导，正是在张老师的耐心和细心地指导下，才有了今日本论文的研究工作，感谢恩师。张老师渊博的知识，勤奋的工作作风，独立思考的能力以及他朴实无华，平易近人的人格魅力，为我树立了为人为学的榜样。同时，张老师为我们提供了良好的学习和科研环境，使我能在实验室充实而快乐的度过我的研究生生涯。在攻读硕士学位的三年中，无论是在学业上，还是在生活上，张老师都对我精心指导。在找工作时，张老师也给了我很多的意见和建议。在此，向张老师表示诚挚的谢意和最深的敬意。学生让你费心了。

同时感谢实验室的杨俊坡，李路阳，杜永光，张刘飘，感谢他们对我论文的指导和在排版方面给予的帮助，使论文能够很好的完成。

我还要感谢我的师姐刘晓庆，感谢她在工作方面给予的鼓励和意见，她虽然毕业了，但她永远是我们大姐姐。

非常的感谢实验室的师兄师姐和师弟师妹们，他们是：李路阳，杨俊坡，刘晓庆，解春雷，张刘飘，刘威，张特，蒋福强，张福健，边康龙，杜永光等；和他们朝夕相处，如同生活在一个大家庭中，与他们无拘无束的交流和讨论，让我收获良多，他们的敏锐洞察力和他们的提出的问题时常给我激励和启发。与他们在一起，收获的不仅是学业上的进步，更是深挚的友谊。

非常的感谢我的舍友和朋友们在生活和学习上对我的帮助和宽容，和她们这两年的生活，我非常开心，从她们身上我也学到了很多东西。她们是：杨依灿，乔巧梅，韩建飞，胡江莹，张蕾，赵芳。

深深地感谢我的父母，这么多年以来他们含辛茹苦，任劳任怨，支持我的学业。同时也非常感谢的弟弟，弟弟虽然比我小，但有时候却像个哥哥，在我不开心时会鼓励我，开导我，我能完成学业与他们在物质上的支持和精神上的鼓励是分不开的。

最后，感谢所有关心，爱护，帮助和启发过我的人。

参考文献

[1] Shannon C E. Communication theory of secrecy systems, Bell System Technical Journal, 1949, 28(4): 656-715.

[2] Meier W. and Staffelbach O. Nonlinearity criteria for cryptographic function, In Advances In Cryptology-EURCRYPT 89, VOLUME 434 of LNCS, pp. 549-562, Springer- Verlag, 1990.

[3] Nyberg K., Differentially uniform mappings for cryptography. In Advances in Cryptology-EUROCRYPT 93, VOLUME 765 of LNCS, pp. 55-64, Springer- Verlag, 1993.

[4] Preneel B, Leekwijck w.v, Linden L.V. , et al., Propagation characteristics of Boolean function , In Advances in Cryptology-EUROCRYPT 90, volume 473 of LNCS, pp. 161-173, Springer-Verlag, 1991.

[5] Siegenthaler T.: Correlation immunity of nonlinear combing function for cryptographic applications, IEEE Transactions on Information theory, volume 30, no 5, pp. 776-780, 1984.

[6] Courtois N, Meier W. Algebraic attacks on stream ciphers with linear feedback [C]. EUROCRYPT 2003, LNCS 2729. Springer-Verlag, 2003: 179-194.

[7] Meier W, Pasalic E, Carlet C, Algebraic attacks and decomposition of Boolean function. In: Advances in Cryptology-EUROCRYPT 2004 .Lecture Notes in computer Science, volume.3027. Springer,Berlin, pp. 474-491(2004).

[8] Courtois N, Meier W. Algebraic attacks on stream ciphers with linear feedback. In: EUROCRYPT 2003. Lecture Notes in computer Science, volume. 2656. Spring, Berlin, pp. 474-491(2004).

[9] Carlet C, Dalai D, Gupta K, Maitra S. Algebraic immunity for cryptographically significant Boolean function: analysis and construction. IEEE Transactions on Information Theory, 52, 3105-3121(2006).

[10] Dalai D, Maitra S. Reducing the number of homogeneous linear equations in finding annihilators. In: Sequences and Their Applications 2006.Lecture Notes in Computer Science , volume 4086. Springer, Berlin, pp.376-390(2006).

[11] Dalai D, Gupta K, Maitra S.:Cryptographically significant Boolean function: co-nstruction and analysis in terms of algebraic immunity .In: Workshop on Fast Soft ware Encryption, FSE 2005. Lecture Notes in Computer Science, volume 3557. Springer, Berlin, pp. 98-111(2005).

[12] Dalai D, Gupta K, Maitra S.: Notion of algebraic immunity and its evaluation related to fast algebraic attacks .In: Second International Workshop on Boolean functions : Cr- y ptography and Applications, BFCA 2006, Cryptology ePrint Archive, Report 2006/01 8, pdf.

[13] Feng K, Liao Q, Yang J.: Maximal value of generalized algebraic immunity. Des -igns Codes Cryptography. 50, 243-252(2009).

[14] Meier W, Staffelbach O.:Fast correlation attacks on stream ciphers. In: Advances in Cryptology-EUROCRYPT 2004. Lecture Notes in Computer Sciences, volume 330. Springer, Berlin, pp. 301-314(1988).

[15] Ding C, Xiao G, Shan W.: The Stability Theory of Stream Ciphers. Springer, Berlin(1991).

[16] Lobanov M.:Tight bound between nonlinearity and algebraic immunity, In: Cryp- tology ePrint Archive, Report 2005/441. http://eprint.iacr.org/2005/441.pdf.

[17] Carlet C, Gaborit P.: On the construction of Boolean functions with a good algebr aic immunity. In: Proceeding of IEEE International Symposium on Information T heory (ISIT) 2005, pp. 1101-1105, 2005.

[18] Carlet C, Feng K.: An infinite class of balanced Boolean function with optimal al- gebraic immunity, good immunity to fast algebraic attacks and good nonlinearity. Volume 5350. Springer, Berlin, pp. 425-440(2008).

[19] Tu Z, Deng Y.: A Conjecture on Binary String and Its Applications on Constructi- ng Boolean function of Optimal Algebraic Immunity. Cryptology ePrint Archive, Report 2009/272, 2009. http://eprint.iacr. Org/2009/272.pdf.

[20] 冯登国. 频谱理论及其在密码学中的应用. 北京：科学出版社，2000.

[21] 李超，屈江龙，周悦. 密码函数的安全性指标分析. 科学出版社，北京，2011.

[22] Xiao Guo-zhen, Massey J L. A Spectral Characterization of Correlation-Immune Combining Functions. IEEE Transaction on Information Theory, 1988, 34(3): 569-571.

[23] 高凌. 弹性布尔函数的构造[D]. 国防科学技术大学，2011.

[24] Webster A F,Tavares S E.On the design of S-boxes. Advance in cryptology-CRYPTO 85 Lecture Notes in Computer Science, Berlin, Heidelberg, New York: Springer-Verlag, 219: 523-534(1986).

[25] Courtios N, Merier W. Algebraic attacks on stream ciphers with linear feedback [C]. EUROCRYPT 2003, LNCS 2656. Springer-Verlag, 2003: 345-359.

[26] 周宇. 布尔函数的密码学性质研究[D]. 西安电子科技大学, 2009.

[27] Sihong S, Xiaohu T, Xiangyong Z.: A systematic method of constructing Boolean functions with optimal algebraic immunity based on the generator matrix of the R -eed Muller code. Designs Codes Cryptography. DOI.10.1007/s10623-01309801- z.

[28] Muller D.:Application of Boolean algebra to switching circuit design and eo error detection. IEEE Transaction on Information Theory. 3, 6-12(1954).

[29] Reed S.: A class of multiple-error-correcting codes and the decoding scheme. IEEE Transaction on Information Theory 4, 38-49(1954).

[30] Dalai D K, Gupta K C, Maira S. Results on Algebraic Immunity for Cryptographically Significant Boolean function[C]//Canteaut A, Viswanathan K eds. INDOCRYPT 2004. Lecture Notes in Computer Science, volume. 3348. Springer, 92-106(2004).

[31] Dong D, Fu S, Qu L, Li C. A new construction of Boolean functions with maximum algebraic immunity. In: ISC 2009. Lecture Notes in Computer Science, volume. 5735. Springer, Berlin, pp. 177-185(2009).

[32] Carlet C.: a Method of construction of balanced functions with optimal algebraic immu –nity. In: International Workshop on Coding and Cryptology, pp. 25-43(2007).

[33] Chen Y, Lu P. Constructions of even-variable Boolean functions with optimal algebraic immunity[EB]. http://eprint .iacr.org/2009/130.

[34] E. Pasalic and T. Johansson, "Further results on the relation between nonlinearity and resiliency of Boolean function " in Proc.IMA Conf. Cryptography and Coding. Ne- w York: Springer-Verlag, 1999, volume, 1746, pp. 35-45.

[35] Dillon J F. Elementary hadamard difference sets[M]. Ph. D. Thesis, University of Maryland, 1974.

[36] H. Dobbertin, Construction of Bent functions and balanced Boolean functions with high nonlinearity, in Proc. Workshop on Fast Software Encryption(FES 1994), Berlin, Germany, 1995, volume. 1008, pp. 61-74.

[37] Zhang Weiguo, and Xiao Guozhen, Constructions of Almost Optimal Resilient Boolean Functions on Large Even Number of Variables, IEEE Transactions on Information Theory , vol. 55, no. 12, 2009, pp. 5822-5831.

研究成果

参加科研情况：

1. 国家自然科学基金：几乎最优弹性密码函数的设计和分析(No.61003299)。
2. ISN 国家驻点实验室课题：广义 Maiorana-McFarland 密码函数构造技术研究。
3.陕西省自然科学技术研究计划项目：同时抵抗多种攻击的密码函数的设计与分析。

附录 A

A1 (8, 0, 6, 112, 3)的真值表：

00110011001110011001011010101100101010100011100101100110111111111000011111010110000111001110011001010110000111100010101011100011011110000100101101001100110101010110000111010010111000110001100110011111000101001111110000000000000011100100111100100110011001 1001

进行变换后 8 元一阶弹性函数后真值表：

01011110010010011011110111111100000010101100011110100010111110000000110000000111001010010001011011111001001000111110100010101101001000010011011110110001001110001011100101011000000011011011010001110111110111001101100110010010100011101101010100101101011010 0001

A2 (10, 0, 8, 472, 4) 的真值表：

5fa509faac3a56aac69336a696ffc36960a395006c565f39a563c53fc33a0fc36f69c3c6aaa5f3666aa095a9a6f9556353995f3963f50f5fa66953056c9a3a50fc90a5f635309faaffcc303563956c96ff3c05365350c99f3305963a3359f0f336f5635560cf5cfa0a6009caa030a033cf06930a30fa3093c0f0663c5aa05c65

进行变换后 10 元一阶弹性函数后真值表：

47f2f5cb420466d65885742c141374e03ff35343874bfa7c2e53f2378646bf2b6c391afa726d6026901d17d1397ae42f4330584156067f99e5c9a5f39da99c9a78f5b40843ab53eedfcdc34de060dcbd839b7504cd5a4c9c3282e0506bb88a57527db3abc26ab928dfde4626a2aed0c648342a9babdbac8b9f6d58090f698596

A3 (10, 0, 8, 482, 4)的真值表：

1e0a916367f7544bf94ec94ee0e4ad06584f2b8d5f9f20a23f7452e1cc3e0a3226e5bffba95a4bf9ee6338b9f4f56433cf932b6295085b9e576544932b4745321ec7c9dc33a272394a8c6cd78415ba90c3316b442f238839cfbbd3879a8fb0a6f3e1e4e8a0e7267f6b54207f8a0d402a9c299277c1db493a12e2c85054c36bab

A4 (12, 0, 10, 1984, 5)的真值表：

68b0eba6e4dc1b5fd1d5e1e0e9378b0f1807faec12df5a1618fcb69b88444193191183a4f0bf52bbab3224d307d9ebf5032fb63fe0a23ae468610b7fdc2d1ca090831e32c55d77c312d0e9e4431489d1de4a872653f6dda2039cb41b5062f6e016ba9cc5f6dec7ebe95d291740a876ba44b09b142ccbadc5846d9630ed7a

33b0c49e435c48a3c2e349a7a02e32adc9921154239606f3ca16aead7eee3e8af00ffbd557a89b84ee6a
fc7f0fca0e7f50e8fba6bd21f6e167eec79e408526269e1e6db3d23af30cc66f1b06416111cf6f9a9fa6
7691b62a36b7909ac5b8f85940bdc78f7ae3274dea4360c13c4e158cfc1858915641f9c3fced9a9364db
47cbe35ed4c13eae5efa72be538905f155d5b624e35ced67b5640f7a281215618235edbba18b7f008986
f5019d8ccb734653cc5a0933d8d2b8cd98b1a127b0b1a85000a57f983d5ee89e84c3e949d38eb4a92c02
8cd1f4ba2053d4e61f2f8556d3520c9624779c47b2543f18792be1a55ee2583e1685c8d2e8c166fafe2e
c898ce8ef88a6df18cab1164fc5d001537ff491cdd42158390a93965a9326c3334dded976d3408215e71
1e99ec487f4307c844bee700638a7ae68a80b031fcc945baad3f8b6b4aaf85dbdffc1b2b698c54c6f553
e7b91b4d7444a3809ac1710698253209c1eeb28e5355c0d4b9f072fceae6e523959f4443d874faffb560
f5b50cc5d075d681